[Logo der Organisation]

[Name der Organisation]

INFORMATIONSSICHERHEITSPOLITIK

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

Commented [27A1]: Um zu erlernen, wie Sie dieses Dokument ausfüllen und echte Beispiele darüber zu sehen, was Sie schreiben müssen, schauen Sie sich dieses Video-Tutorial an:
"How to Write the ISMS Policy According to ISO 27001".

Um auf das Tutorial zuzugreifen: Suchen Sie in Ihrem Posteingang die E-Mail, die Sie zum Zeitpunkt des Kaufes erhalten haben. Dort finden Sie einen Link und ein Passwort, mit denen Sie auf das Video-Tutorial zugreifen können.

Commented [27A2]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A3]: Dieser Artikel hilft Ihnen, den Inhalt der Informationssicherheitspolitik zu verstehen:

What should you write in your Information Security Policy according to ISO 27001?
https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/

Commented [27A4]: Dieser Artikel hilft Ihnen den Zweck der Informationssicherheitspolitik zu verstehen:

Informationssicherheitspolitik – wie detailliert sollte sie sein?
https://advisera.com/27001academy/de/blog/2011/03/25/informationssicherheitsleitlinie-wie-detailliert-sollte-sie-sein/

Commented [27A5]: Wenn Sie ein Dokument mit detaillierten Regeln der Informationssicherheit benötigen, verwenden Sie bitte die im Toolkit inkludierte IT-Sicherheitspolitik.

Sie können die IT-Sicherheitspolitik auch separat hier kaufen:
https://advisera.com/27001academy/de/documentation/it-sicherheitspolitik/

Commented [27A6]: 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

Zielsetzung dieser auf oberster Ebene angesiedelten Politik ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für Informationssicherheits-Management.

Diese Politik wird auf das gesamte Informationssicherheits-Managementsystem (ISMS) angewendet, und wie im Dokument zum ISMS Anwendungsbereich definiert.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation], sowie relevante externe Parteien.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte 5.2 und 5.3
- Dokument zum ISMS Anwendungsbereich
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen
- *
- [Verfahren zum Management von Informationssicherheits-Vorfällen]

Commented [27A7]: Hier alle internen Dokumente der Organisation auflisten, die mit dieser Richtlinie zusammenhängen, z.B. Geschäftsstrategie, Geschäfts-Entwicklungsplan, Strategisches Risikomanagement, usw.

Commented [27A8]: Siehe Punkt 4.5

3. Informationssicherheit: Grundbegriffe

Vertraulichkeit – die Eigenschaft von Informationen, dass sie lediglich berechtigten Personen oder [illegible]

[illegible]

[illegible]
zugänglich sind, wenn ein solcher Zugang notwendig ist

[illegible]

[illegible]
Informationssicherheit befasst

4. Verwaltung der Informationssicherheit

4.1. Zielvorgaben und Messung

Die generellen Zielvorgaben des Informationssicherheits-Managementsystems sind die folgenden:

[redacted]

Zielvorgaben und für die Definition neuer Zielvorgaben verantwortlich.

[redacted]

und von [Stellenbezeichnung] im Rahmen der Erklärung zur Anwendbarkeit genehmigt.

Alle diese Zielvorgaben müssen mindestens einmal jährlich überprüft werden.

[redacted]

[Stellenbezeichnung] analysiert und evaluiert die Messresultate und berichtet anschließend an [redacted]

4.2. Anforderungen an Informationssicherheit

Diese Richtlinie und das gesamte ISMS müssen sowohl den rechtlichen und gesetzlichen [redacted]

[redacted]

rechtlichen, amtlichen und vertraglichen Verpflichtungen bereitgestellt.

4.3. Maßnahmen zur Informationssicherheit

[redacted]

Anwendbarkeit aufgeführt.

4.4. Verantwortlichkeiten

Folgendes sind die grundsätzlichen Verantwortlichkeiten für das ISMS:

- [redacted]
- [redacted] die Berichterstattung über dessen Leistungsfähigkeit.
- [redacted]

Commented [27A9]: Falls notwendig, ändern und/oder andere [redacted]

Commented [27A10]: Weitere Informationen zur Abstimmung zwischen ISO 27001 und dem Unternehmen finden Sie in diesem Artikel:

Aligning information security with the strategic direction of a company according to ISO 27001 https://advisera.com/27001academy/blog/2017/02/20/strategic-direction-of-a-company-according-to-iso-27001/

Commented [27A11]: Informationen zur Bedeutung von Kontrollzielen finden Sie in diesem Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [27A12]: Prüfen, ob diese Häufigkeit angemessen ist.

Commented [27A13]: Sie finden diese Vorlage im Ordner " Managementbewertung ".

Commented [27A14]: Hier auch andere Bereiche auflisten, die [redacted]

Commented [27A15]: Um die Verantwortlichkeiten des Top-Managements besser zu verstehen, lesen Sie diesen Artikel:

Roles and responsibilities of top management in ISO 27001 and ISO 22301 https://advisera.com/27001academy/blog/2014/06/09/roles-and-responsibilities-of-top-management-in-iso-27001-and-iso-22301/

Commented [27A16]: Mitglied der Unternehmensleitung.

Commented [27A17]: Eine oder mehrere Personen; [redacted]

Commented [27A18]: Dies muss das Leitungs-Organ der [redacted]

Überprüfung durch das Management ist der Nachweis der Angemessenheit, Eignung und [illegible]

- [illegible]
- Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der Werte unterliegt der Verantwortung des Eigentümers der jeweiligen Werte.
- [illegible]
- [illegible] kommuniziert werden, durch wen und wann.
- [Stellenbezeichnung] ist für die Aufstellung und Implementierung des Plans für Training und [illegible]

Commented [27A19]: Verschiedene Personen können entsprechend der Arten von Vorfällen benannt werden.

Commented [27A20]: Oder hier auf das Verfahren für die Behandlung von Vorfällen verweisen.

Commented [27A21]: Diese Schulung hilft Ihnen, die Mitarbeiter zu schulen, das Sicherheitsbewusstsein zu steigern und ihr Wissen zu verfolgen: https://training.advisera.com/awareness-session/security-awareness-training/

4.5. Politik-Kommunikation

[illegible]

5. Unterstützung der ISMS Umsetzung

[illegible] Weiterverbesserung mit geeigneten Ressourcen unterstützt werden, um alle in dieser Politik genannten Zielvorgaben zu erfüllen.

Commented [27A22]: Um ein besseres Verständnis der Ressourcenbereitstellung zu erhalten, lesen Sie diesen Artikel:

How to demonstrate resource provision in ISO 27001 https://advisera.com/27001academy/blog/2017/04/10/how-to-demonstrate-resource-provision-in-iso-27001/

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 [27A23]: Dies ist lediglich eine Empfehlung. Häufigkeit nach Bedarf anpassen.

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

- [illegible]
- [illegible]
- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

[Unterschrift]

Commented [27A24]: Die Politik muss vom Leitungsorgan der Organisation innerhalb des ISMS Anwendungsbereiches genehmigt werden.

Commented [27A25]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.