[Logo der Organisation]

[Name der Organisation]

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

RICHTLINIE ZUR KLASSIFIZIERUNG VON INFORMATIONEN

Commented [27A2]: Um mehr darüber zu erfahren, wie Informationen zu klassifizieren sind, lesen Sie diesen Artikel:

Information classification according to ISO 27001
https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

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

Commented [27A3]: 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.

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Änderungs-Historie

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

Inhaltsverzeichnis

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist sicherzustellen, dass Informationen auf einem angemessenen Niveau geschützt sind.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Arten von Information, unabhängig von deren Form – Papier oder elektronische Dokumente, Anwendungen und Datenbanken, persönliches Wissen, etc.

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

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Informationssicherheitspolitik
- Bericht zur Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Inventar der Werte
- Liste gesetzlicher, amtlicher, vertraglicher und anderer Verpflichtungen
- Verfahren zum Umgang mit Informationssicherheits-Vorfällen
- [Sicherheitsverfahren für die IT-Abteilung] / [Richtlinie zu Entsorgung, Vernichtung und Weiterverwendung]
- IT-Sicherheitspolitik

Commented [27A4]: Sollten Sie über diese Liste nicht verfügen, dann fügen Sie hier einfach weitere Aufzählungspunkte mit den sich auf die Klassifizierung von Informationen beziehenden gesetzlichen Auflagen und vertraglichen Verpflichtungen hinzu.

Commented [27A5]: Hier das Dokument auswählen in welchem die sichere Löschung von Daten vorgeschrieben wird.

3. Klassifizierte Information

3.1. Umsetzungsschritte und Verantwortlichkeiten

Folgendes sind die Umsetzungsschritte und Verantwortlichkeiten für Informationsmanagement:

Bezeichnung des Umsetzungsschrittes	***Verantwortlichkeit***
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Falls klassifizierte Informationen von außerhalb der Organisation empfangen werden, ist [illegible] für deren Klassifizierung entsprechend der Vorgaben dieser Richtlinie verantwortlich und diese Person wird zum Eigentümer dieses Informationswertes.

3.2. Klassifizierung von Information

3.2.1. Klassifizierungskriterien

Die Vertraulichkeitsstufe wird auf Basis folgender Kriterien festgelegt:

- [illegible] - basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen
- [illegible] - basierend auf dem für jede Information
während der Risikoeinschätzung kalkulierten höchsten Risiko
- [illegible] - basierend auf den (zum gesetzlichen, amtlichen, vertraglichen und anderen Verpflichtungen

3.2.2. Vertraulichkeitsstufen

Alle Informationen müssen nach Vertraulichkeitsstufen klassifiziert werden.

Vertraulichkeitsstufe	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Commented [27A6]: Vertraulichkeitsstufen und Kennzeichnungen können an das in der Organisation bestehende Schema, an die ortsübliche Systematik oder an ein durch Rechtsvorschriften vorgegebenes Schema angepasst werden.

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Um unnötige Kosten für den Schutz von Informationen zu vermeiden gilt die Grundregel, dass die

3.2.3. Liste berechtigter Personen

Information mit der Klassifizierung „Eingeschränkt“ und „Vertraulich“ muss immer von einer Liste

haben.

3.2.4. Re-Klassifizierung

Die Eigentümer der Werte müssen die Vertraulichkeitsstufe ihrer Informationswerte alle [zwei Jahre]

Commented [27A7]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

3.3. Kennzeichnung von Information

Die Kennzeichnung mit Vertraulichkeitsstufen wird folgendermaßen durchgeführt:

- Aktenordner angegeben, in dem das Dokument abgelegt ist
- **Elektronische Dokumente** - die Vertraulichkeitsstufe wird in der oberen rechten Ecke jeder
- wird
- **Elektronische Post** - die Vertraulichkeitsstufe wird in der ersten Zeile des E-Mail Inhaltes
- **Mündlich weitergegebene Information** - die Vertraulichkeitsstufe vertraulicher Information, die in persönlichen Gesprächen, über Telefon oder andere Kommunikationsarten

3.4. Umgang mit klassifizierter Information

Commented [27A8]: Alle hier genannten Regeln sollten an die Anforderungen der Organisation angepasst werden.

Alle Personen mit Zugang zu klassifizierter Information müssen die in folgender Tabelle aufgelisteten

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Vorfall betreffend des Umgangs mit klassifizierter Information muss entsprechend des Verfahrens zum Umgang mit Informationssicherheits-Vorfällen gemeldet werden.

Informationseigner dürfen den Bereich der Organisation nur verlassen, wenn dafür eine Genehmigung entsprechend der IT-Sicherheitspolitik erteilt wurde.

Die Methode für sichere Löschung und Vernichtung von Datenträgern wird im Dokument Sicherheitsverfahren für das IT-Abteilung | Richtlinie zu Entsorgung, Vernichtung und Weiterverwendung eingegeben.

	Interner Gebrauch	*Eingeschränkt**	*Vertraulich**
Papier-Dokumente	• Nur berechtigte Personen erhalten Zugang • Bei Versand außerhalb der Organisation muss das Dokument als Einschreiben versandt werden • Dokumente dürfen auch nur in Räumen aufbewahrt werden, zu denen die Allgemeinheit keinen Zugang hat • Die Dokumente müssen regelmäßig von Druckern und Faxgeräten entfernt werden	• Das Dokument muss in einem verschlossenen Schrank aufbewahrt werden • Dokumente dürfen innerhalb und außerhalb der Organisation nur in einem verschlossenen Umschlag übertragen werden • Für den Versand außerhalb des Organisationsbereichs muss die Versandart Einschreiben mit Rückschein gewählt werden • Die Dokumente müssen unmittelbar von Druckern und Faxgeräten entfernt werden • Nur der Eigentümer des Dokuments darf es kopieren • Nur der Eigentümer des Dokuments darf es vernichten	• Das Dokument muss in einem Tresor aufbewahrt werden • Das Dokument darf innerhalb und außerhalb der Organisation nur durch eine vertrauenswürdige Person, und in einem verschlossenen und versiegelten Umschlag übergeben werden • Versand des Dokuments per Fax ist nicht erlaubt • Das Dokument darf nur ausgedruckt werden wenn die berechtigte Person sich direkt am Drucker befindet
Elektronische Dokumente	• Nur berechtigte Personen erhalten	• Nur Personen mit Zugangsberechtigung	• Das Dokument muss verschlüsselt

Commented [27A9]: Diesen Absatz löschen, falls Maßnahme A.11.2.5 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A10]: Hier das Dokument auswählen, mit dem die sichere Löschung von Daten vorgeschrieben wird.

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

	Zugang • [illegible] • [illegible] dem das Dokument gespeichert ist, muss [illegible] • [illegible] gesperrt werden	g für das Dokument dürfen Zugang zu dem Teil des Informations-[illegible] • [illegible] • [illegible]	gespeichert werden • Das Dokument darf nur auf Servern [illegible] • [illegible]
[illegible]	• Nur berechtigte Personen dürfen Zugang erhalten • [illegible] • [illegible] • [illegible]	• Anwender müssen sich vom Informationssystem [illegible] • [illegible]	• Für die Zugangssteuerung [illegible] • Das Informations-System darf ausschließlich auf [illegible] • [illegible] denen die Identität von Personen vor

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

			dem Zutritt überprüft wird
Elektronische Post	• Nur berechtigte [illegible] • [illegible] • [illegible] genannten Regeln gelten	• Der Versand von E-[illegible]	• [illegible]
[illegible]	• Nur berechtigte Personen dürfen Zugang [illegible] • [illegible] • [illegible] • [illegible] nur in Räumen mit überwachtem [illegible] aufbewahrt werden	• Datenträger und Dateien müssen verschlüsselt sein • [illegible] • [illegible] der Datenträger als Einschreiben mit [illegible] • [illegible] oder vernichten	• Datenträger müssen in einem Tresor [illegible] • [illegible]
Mündlich [illegible]	• Nur berechtigte [illegible] • [illegible] Information kommuniziert wird	• Die Räumlichkeit muss schalldicht sein • [illegible]	• Besprechungen, die [illegible] • [illegible] erlaubt

*Maßnahmen verstehen sich kumulativ. Das heißt, Maßnahmen jeglicher Vertraulichkeitsstufe [illegible]

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden

Name der Aufzeichnung	*Aufbewahrungs-Ort*	*Verantwortlicher für Aufbewahrung*	*Maßnahme zum Schutz der Aufzeichnung*	*Aufbewahrungs-Dauer*
[Liste der berechtigten Personen für den Zugang zu Dokumenten]	Zusammen mit der Information in der die Vertraulichkeits-stufe angegeben ist	Eigentümer des Informations-Wertes	Selbe Maßnahme wie diejenige zum Schutz der Information	Die Liste muss so lange aufbewahrt werden, wie die zugehörige Information vorhanden ist

Commented [27A11]: Bitte ändern Sie diese Aufzeichnung derart, dass sie zu denen passt, die Sie bereits in Ihrem Unternehmen haben. Sollten Sie keine ähnliche Aufzeichnung haben, können Sie eine neue Aufzeichnung in einem neuen Format erstellen, welches Ihnen am besten zusagt.

5. 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 [27A12]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A13]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.