[Logo der Organisation]

[Name der Organisation]

RICHTLINIE ZUR KLASSIFIZIERUNG VON INFORMATIONEN

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

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

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/

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.

©2019 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

1. ZWECK, ANWENDUNGSBEREICH UND ANWENDER 3

2. REFERENZDOKUMENTE 3

3. KLASSIFIZIERTE INFORMATION 3

3.1. UMSETZUNGSSCHRITTE UND VERANTWORTLICHKEITEN 3

3.2. KLASSIFIZIERUNG VON INFORMATION 4

3.2.1. Klassifizierungskriterien 4

3.2.2. Vertraulichkeitsstufen 4

3.2.3. Liste berechtigter Personen 5

3.2.4. Re-Klassifizierung 5

3.3. KENNZEICHNUNG VON INFORMATION 5

3.4. UMGANG MIT KLASSIFIZIERTER INFORMATION 5

4. VERWALTUNG VON AUFZEICHNUNGEN DIE ZU DIESEM DOKUMENT ERSTELLT WURDEN 9

5. GÜLTIGKEIT UND DOKUMENTEN-HANDHABUNG 9

©2019 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]

©2019 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]

3.2. Klassifizierung von Information

3.2.1. Klassifizierungskriterien

Die Vertraulichkeitsstufe wird auf Basis folgender Kriterien festgelegt:

- Wert der Information – basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen
- [illegible]
- [illegible]

3.2.2. Vertraulichkeitsstufen

Alle Informationen müssen nach Vertraulichkeitsstufen klassifiziert werden.

Vertraulichkeitsstufe	*Kennzeichnung*	*Klassifizierungskriterien*	*Zugangsbeschränkung*
Öffentlich	(nicht gekennzeichnet)	[illegible]	[illegible]
Interner Gebrauch	INTERNER GEBRAUCH	[illegible]	[illegible]
Eingeschränkt	EINGESCHRÄNKT	[illegible]	[illegible]
Vertraulich	VERTRAULICH	[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.

©2019 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 niedrigste Vertraulichkeitsstufe genutzt wird, die einen geeigneten Schutz bietet.

3.2.3. Liste berechtigter Personen

Information mit der Klassifizierung „Eingeschränkt“ und „Vertraulich“ muss immer von einer Liste [redacted] Organisation Zugang zu einem solchen Dokument haben.

3.2.4. Re-Klassifizierung

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

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

3.3. Kennzeichnung von Information

Die Kennzeichnung mit Vertraulichkeitsstufen wird folgendermaßen durchgeführt:

- **Papierdokumente** – die Vertraulichkeitsstufe wird in der oberen rechten Ecke jeder Seite des Dokuments angegeben; ebenso wird sie auf der Vorderseite des Deckblattes sowie auf dem Aktenordner angegeben, in dem das Dokument abgelegt ist
- [redacted]
- [redacted]
- [redacted]
- **Elektronische Datenträger** (Disketten, Speicherkarten, etc.) - die Vertraulichkeitsstufe muss auf der Oberfläche eines solchen Mediums angegeben werden
- **Mündlich weitergegebene Information** - die Vertraulichkeitsstufe vertraulicher Information, [redacted]

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 [redacted]

©2019 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.

[redacted]

[redacted]

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.

	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 sich nur in Räumen befinden zu denen die Allgemeinheit keinen Zugang hat • Die Dokumente müssen regelmäßig von Druckern und Faxgeräten entfernt werden	[redacted]	[redacted]
Elektronische Dokumente	• Nur berechtigte Personen erhalten	[redacted]	[redacted]

©2019 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

	Zugang • Beim Austausch von Dateien über Dienste wie FTP, Instant Messaging, etc., müssen sie passwortgeschützt sein • Der Zugang zum Informationssystem in dem das Dokument gespeichert ist, muss durch ein sicheres Passwort geschützt sein • Der Bildschirm auf dem das Dokument angezeigt wird, muss automatisch nach [Nummer] Minuten Inaktivität gesperrt werden	[illegible]	[illegible]
Informations-Systeme	[illegible]	[illegible]	[illegible]

©2019 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

			[illegible]
Elektronische Post	• Nur berechtigte Personen dürfen Zugang erhalten • Der Absender muss die Empfängeradresse sorgfältig prüfen • Alle unter „Informationssysteme“ genannten Regeln gelten	[illegible]	[illegible]
Elektronische Datenträger	• Nur berechtigte Personen dürfen Zugang erhalten • Datenträger oder Dateien müssen passwortgeschützt sein • Bei Versand außerhalb der Organisation muss der Datenträger als Einschreiben versandt werden • Der Datenträger darf nur in Räumen mit überwachtem physikalischem Zugang aufbewahrt werden	[illegible]	[illegible]
Mündlich weitergegebene Information	• Nur berechtigte Personen dürfen Zugang zur Information erhalten • Nicht berechtigte Personen dürfen sich nicht im selben Raum aufhalten, während die Information kommuniziert wird	[illegible]	[illegible]

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

©2019 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

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 [27A11]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

- [redacted]
- [redacted]

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A12]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.

©2019 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.