[Logo der Organisation]

[Name der Organisation]

Commented [EU GDPR1]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

RICHTLINIE ZUR KLASSIFIZIERUNG VON INFORMATIONEN

Commented [EU GDPR2]: 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 [EU GDPR3]: 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.

©2017 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
TT.MM.JJJJ	0.1	EUGDPRAcademy	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 8

5. GÜLTIGKEIT UND DOKUMENTEN-HANDHABUNG 9

©2017 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 (einschließlich personenbezogener Daten), 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
- Reaktion auf eine Datenschutzverletzung und Meldeverfahren
- [Sicherheitsverfahren der IT-Abteilung] / [Politik zur Entsorgung und Vernichtung]
- IT-Sicherheitspolitik

Commented [EU GDPR4]: 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 [EU GDPR5]: 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]

©2017 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 [Stellenbezeichnung] 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:

- Wert der Information – basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen
- [Sensibilität und Kritikalität der Information – basierend auf dem für jede Information während der Risikoeinschätzung kalkulierten höchsten Risiko]
- [Rechtliche und vertragliche Verpflichtungen – basierend auf den (Link gesetzlichen, amtlichen, vertraglichen und anderen Verpflichtungen]

3.2.2. Vertraulichkeitsstufen

Alle Informationen müssen nach Vertraulichkeitsstufen klassifiziert werden.

Vertraulichkeitsstufe	***Kennzeichnung***	***Klassifizierungskriterien***	***Zugangsbeschränkung***
Öffentlich	(nicht gekennzeichnet)	Die Veröffentlichung der Information würde die Organisation auf keine Weise beeinträchtigen	Information ist öffentlich verfügbar
Interner Gebrauch	INTERNER GEBRAUCH	Unberechtigter Zugang zur [Information könnte geringen Schaden und/oder Unannehmlichkeiten für die Organisation verursachen]	Information ist für alle Mitarbeiter und ausgesuchte Dritte verfügbar
[Vertraulich]	[VERTRAULICH]	Unberechtigter Zugang zur [Information könnte erheblichen Schaden für das Geschäft und/oder das Ansehen der Organisation verursachen]	[Information ist nur einer spezifischen Gruppe von Mitarbeitern und externen Dritten zugänglich]
[Vertraulich]	[VERTRAULICH]	Unberechtigter Zugang zur [Information könnte katastrophalen (irreparablen) Schaden für das Geschäft und/oder das Ansehen der Organisation verursachen]	[Information ist nur einzelnen Mitarbeitern der Organisation zugänglich]

Commented [EU GDPR6]: Vertraulichkeitsstufen und Kennzeichnungen können an das in der Organisation bestehende Schema, an die ortsübliche Systematik oder an ein durch Rechtsvorschriften vorgegebenes Schema angepasst werden.

©2017 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 [illegible] begleitet werden, in welcher der Eigentümer der Information die Namen oder Stellenbezeichnungen der Personen spezifiziert, die Zugangsberechtigung zu dieser Information haben.

Dieselbe Regel gilt für die Vertraulichkeitsstufe “Interner Gebrauch”, falls Personen außerhalb der Organisation Zugang zu einem solchen Dokument haben.

3.2.4. Re-Klassifizierung

[illegible] Die Eigentümer der Werte müssen die Vertraulichkeitsstufe ihrer Informationswerte alle [illegible] überprüfen und bewerten, ob die Vertraulichkeitsstufe geändert werden kann. Falls möglich, sollte die Vertraulichkeitsstufe herabgesetzt werden.

Commented [EU GDPR7]: 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
- **Elektronische Dokumente** – die Vertraulichkeitsstufe wird in der oberen rechten Ecke jeder Seite des Dokuments angegeben
- **Informationssysteme** – die Vertraulichkeitsstufe in Applikationen und Datenbanken wird auf dem Zugangsbildschirm zum System angegeben, ebenso wie in der oberen rechten Ecke jedes darauffolgenden Bildschirmabschnittes, mit dem vertrauliche Information angezeigt wird
- **Elektronische Post** - die Vertraulichkeitsstufe wird in der ersten Zeile des E-Mail Inhaltes angegeben
- **Elektronische Datenträger** (Diskette, Speicherkarten, etc.) – die Vertraulichkeitsstufe muss auf der Oberfläche eines solchen Mediums angegeben werden
- **Mündlich weitergegebene Information** – die Vertraulichkeitsstufe vertraulicher Information, die in persönlichen Gesprächen, über Telefon oder anderen Kommunikationsarten ausgetauscht wird, muss vor der eigentlichen Information mitgeteilt werden

3.4. Umgang mit klassifizierter Information

Commented [EU GDPR8]: 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 Regeln befolgen. [Stellenbezeichnung] muss disziplinarische Maßnahmen einleiten, falls die Regeln [illegible] nicht befolgt werden oder die Information an nicht berechtigte Personen kommuniziert wird. Jeder Vorfall betreffend des Umgangs mit klassifizierter Information muss entsprechend der Reaktion auf eine Datenschutzverletzung und Meldeverfahren gemeldet werden.

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Informationswerte 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 der IT-Abteilung] / [Politik zur Entsorgung und Vernichtung] vorgegeben.

Commented [EU GDPR9]: Diesen Absatz löschen, falls Maßnahme A.11.2.5 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [EU GDPR10]: Hier das Dokument auswählen, mit dem die sichere Löschung von Daten vorgeschrieben wird.

	Interner Gebrauch	*Eingeschränkt**	*Vertraulich**
Papier-Dokumente	• Nur berechtigte Personen erhalten Zugang • [illegible] • [illegible] • [illegible]	• Das Dokument muss in einem verschlossenen Schrank aufbewahrt werden • [illegible] • [illegible] • [illegible] • [illegible] • [illegible]	• Das Dokument muss in einem Tresor aufbewahrt werden • [illegible] • [illegible] • [illegible]
[illegible]	• Nur berechtigte Personen erhalten Zugang • Beim Austausch von Dateien über Dienste	• Nur Personen mit Zugangsberechtigung für das Dokument dürfen Zugang zu dem Teil des	• Das Dokument muss verschlüsselt gespeichert werden • Das Dokument darf nur auf Servern

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

	wie FTP, Instant Messaging, etc., müssen sie passwortgeschützt sein • [redacted]	Informations-Systems erhalten, in dem dieses Dokument hinterlegt ist • [redacted]	gespeichert werden, die unter der Leitung der Organisation stehen • Das Dokument darf nicht über Dienste wie FTP, Instant Messaging, etc. ausgetauscht werden
[redacted]	• Nur berechtigte Personen dürfen Zugang erhalten • [redacted]	• Anwender müssen sich vom Informationssystem abmelden, falls sie sich vom Arbeitsplatz vorübergehend oder dauerhaft entfernen • [redacted]	• Für die Zugangssteuerung zur Information muss ein Authentisierungs-Prozess auf Basis von [redacted] • [redacted]
Elektronische	• Nur berechtigte	• Der Versand von E-	• Alle E-Mails müssen

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Post	Personen dürfen Zugang erhalten • Der Absender muss die Empfängeradresse sorgfältig prüfen • Alle unter „Informationssysteme“ genannten Regeln gelten	Mail außerhalb der Organisation muss verschlüsselt erfolgen	verschlüsselt sein
Elektronische Datenträger	• Nur berechtigte Personen dürfen Zugang erhalten • [illegible] • [illegible] • [illegible]	• Datenträger und Dateien müssen verschlüsselt sein • [illegible] • [illegible] • [illegible]	• Datenträger müssen in einem Tresor aufbewahrt werden • [illegible]
Mündlich weitergegebene Information	• Nur berechtigte Personen dürfen Zugang zur Information erhalten • [illegible]	• Die Räumlichkeit muss schalldicht sein • Die Unterredung darf nicht aufgezeichnet werden	• Besprechungen, die mit jeglicher Art von [illegible] • [illegible]

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

4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

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 [EU GDPR11]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

- Anzahl an Vorfällen im Zusammenhang mit unberechtigtem Zugang zu Informationen
- Anzahl an Informationswerten die mit einer nicht angemessenen Vertraulichkeitsstufe klassifiziert wurden

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [EU GDPR12]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.