[Logo der Organisation]

[Name der Organisation]

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

VERFAHREN ZUM VORFALLSMANAGEMENT

Commented [27A2]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diese Artikel:

- How to handle incidents according to ISO 27001 A.16 https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/
- Using ITIL to implement ISO 27001 incident management https://advisera.com/27001academy/blog/2015/11/10/using-itil-to-implement-iso-27001-incident-management/

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.

Änderungs-Historie

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

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Zweck dieses Dokuments ist die schnelle Erkennung von Sicherheitsereignissen und Schwachstellen sowie die schnelle Reaktion und Antwort auf Sicherheitsvorfälle.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Mitarbeiter und andere Werte, die innerhalb des ISMS Anwendungsbereiches im Einsatz sind, ebenso wie für Lieferanten oder andere Personen außerhalb der Organisation, die mit Systemen und Informationen innerhalb des ISMS Anwendungsbereiches in Berührung kommen.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation], sowie alle oben genannten Personen.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
- Informationssicherheitspolitik
- [Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen]

Commented [27A4]: Falls Sie diese Liste nicht verfügbar haben, können Sie hier weitere Aufzählungspunkte mit den Gesetzvorgaben und Verträgen, die Anforderungen bezüglich des Vorfallsmanagements beinhalten, hinzufügen.

3. Vorfallsmanagement

Ein Informationssicherheits-Vorfall ist "ein einzelnes oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird (ISO/IEC 27000:2009)“.

3.1. Entgegennahme und Klassifizierung von Vorfällen, Schwachstellen und Ereignissen

Jeder Mitarbeiter, Lieferant oder andere Dritte, der in Kontakt zu Informationen und/oder Systemen von [Name der Organisation] steht, muss jegliche Systemschwachstellen, Vorfälle oder Ereignisse, die zu einem möglichen Sicherheitsvorfall führen könnten, folgendermaßen melden:

1. [illegible]
2. [illegible]

[illegible]

Commented [27A5]: Andere eingesetzte Systeme für das Melden von Vorfällen können hinzugefügt werden (z.B. Helpdesk-Anwendungen, usw.)

Der Empfänger der Information muss diese wie folgt klassifizieren:

a) Sicherheitsschwachstelle oder Ereignis – es ist kein Vorfall aufgetreten, jedoch könnte das mit einem System, Prozess oder einer Organisation in Zusammenhang stehende Ereignis in naher oder ferner Zukunft einen Vorfall zur Folge haben

b) [redacted]

c) [redacted]

3.2. Behandlungsverfahren bei Sicherheitsschwachstellen oder -ereignissen

Der Empfänger der Information zu einer Sicherheitsschwachstelle oder einem Ereignis analysiert die Information, stellt die Ursache fest und schlägt gegebenenfalls Vorbeugungs- und Korrektur-Maßnahmen vor.

3.3. Behandlung geringer Vorfälle

Wenn ein geringer Vorfall gemeldet wird, muss der Empfänger der Information folgende Schritte durchführen:

1. Maßnahmen zur Eingrenzung des Vorfalles einleiten
2. [redacted]
3. [redacted]
4. [redacted]

Der Empfänger der Information zu einem geringen Vorfall muss diesen Vorfall protokollieren [die Art seiner Aufzeichnung beschreiben – manuell, elektronisch, automatisiert (z.B. über Helpdesk-Anwendungen)].

3.4. Behandlung erheblicher Vorfälle

Im Fall von erheblichen Vorfällen, die den Betrieb für eine inakzeptable Zeitperiode unterbrechen [redacted]

Commented [27A6]: Falls kein solches Dokument vorhanden ist, hier das Verfahren im Fall eines erheblichen Vorfalls beschreiben.

3.5. Lernen aus Vorfällen

Commented [27A7]: Diesen Punkt löschen, falls Maßnahme A.16.1.6 in der Erklärung zur Anwendbarkeit als nicht anwendbar befunden wurde.

[Stelenbezeichnung] muss alle geringeren Vorfälle vierteljährlich prüfen und jene, die sich wiederholen (oder solche, die sich bei der nächsten Wiederholung zu einem erheblichen Vorfall steigern könnten) im Verzeichnis der Vorfälle vermerken.

[redacted]

3.6. Disziplinarmaßnahmen

[Stellenbezeichnung] muss für jeden Verstoß gegen Sicherheitsregeln ein disziplinarisches Verfahren in die Wege leiten.

Commented [27A8]: Diesen Punkt löschen, falls Maßnahme A.7.2.3 in der Erklärung zur Anwendbarkeit als nicht anwendbar befunden wurde.

3.7. Sammlung von Beweisen

[redacted]

Commented [27A9]: Diesen Punkt löschen, falls Maßnahme A.16.1.7 in der Erklärung zur Anwendbarkeit als nicht anwendbar befunden wurde.

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*
Verzeichnis der Vorfälle	Gemeinsam genutzter Ordner im Intranet	[Stellenbezeichnung]	Nur [Stellenbezeichnung] hat die Berechtigung, das Verzeichnis zu bearbeiten.	3 Jahre

Nur [Stellenbezeichnung] kann anderen Mitarbeitern Zugang zu diesen Aufzeichnungen gewähren.

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

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

Commented [27A10]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

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

6. Anhänge

- Anhang 1 – Verzeichnis der Vorfälle

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A11]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.