Anhang 1 – Vorfallreaktionsplan

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 a Business Continuity Plan According to ISO 22301".

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.

Änderungs-Historie

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

INHALTSVERZEICHNIS

1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Plans ist die Sicherstellung des Schutzes der Gesundheit und Sicherheit der Menschen in einem Katastrophenfall oder bei einem anderen Notfall, sowie die Eindämmung des Notfalls. Die Zielsetzung ist, den Schaden für den Geschäftsbetrieb auf ein Minimum zu begrenzen.

Dieser Plan wird für alle schwerwiegenden Vorfälle angewendet, durch die eine Gefahr besteht, dass irgendeine geschäftskritische Aktivität innerhalb des ISMS [BKMS] Anwendungsbereiches für eine längere Zeitspanne als es die Zielsetzung für den Wiederanlaufzeitpunkt (RPO) zur jeweiligen Aktivität zulässt, unterbrochen werden könnte (im weiteren „Notfall" genannt).

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

Commented [27A2]: Geben Sie bitte den Namen Ihrer Organisation an.

2. Befugnisse und Verantwortlichkeiten im Notfallmanagement

Rolle für die Wiederherstellung / Stellenbezeichnung	***Befugnisse und Verantwortlichkeiten***
Jeder Mitarbeiter	Benachrichtigung der zuständigen Organisationseinheit über den Notfall
[Stellenbezeichnung] oder Mitarbeiter bei [Name der Organisationseinheit]	[illegible]
[illegible]	Alle Schritte zur Aktivierung der Lösungen für die Behebung aller anderen Notfälle
[illegible]	Aktivierung der Wiederherstellungspläne und Lösungen für Aktivitäten
[Stellenbezeichnung]	[illegible]
[Stellenbezeichnung]	Psychologische Hilfe für Mitarbeiter

Commented [27A3]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

Beyond the BCM Manager: Additional roles to consider during the disruptive incident
https://advisera.com/27001academy/blog/2016/12/05/beyond-the-bcm-manager-additional-roles-to-consider-during-the-disruptive-incident/

Commented [27A4]: Z.B.: Leiter der IT-Abteilung

Commented [27A5]: Z.B.: Beauftragter für operative Tätigkeit

Commented [27A6]: Dies muss die im Plan für betriebliches Kontinuitäts-management genannte Person sein.

Commented [27A7]: Siehe auch:

Activation procedures for business continuity plan
http://advisera.com/27001academy/blog/2011/09/26/activation-procedures-for-business-continuity-plan/

Commented [27A8]: Dies muss die im Plan für betriebliches Kontinuitäts-management genannte Person sein.

Commented [27A9]: Muss vom Manager der Personalabteilung/Verantwortlichen benannt werden.

3. Kommunikation

Nachfolgende Tabelle listet die Verantwortlichkeiten für die Kommunikation (dies umfasst sowohl [illegible]

	[Telefon]	[illegible]	[illegible]	[illegible]	*[Medien]*		
[Mitarbeiter]							
[illegible]							
[illegible]							

Commented [27A10]: Dieser Abschnitt sollte um Prozeduren [illegible]

Commented [27A11]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

Enabling communication during disruptive incidents according to ISO 22301
https://advisera.com/27001academy/blog/2016/12/19/enabling-communication-during-disruptive-incidents-according-to-iso-22301/

Commented [27A12]: Verantwortlichkeiten aus der Strategie [illegible]

[Kunden]							
[Interessen-verbände]							

Die Vorgehensweise für die Kommunikation ist folgende:

1. Jeder Mitarbeiter der eine Kommunikationsanfrage erhält oder eine Kommunikation mit interessierten Parteien beginnen will, muss eine solche Anfrage an einen Verantwortlichen entsprechend obiger Auflistung weiterleiten.
2. [illegible]
3. [illegible]
4. [illegible]

Der in obiger Aufstellung genannte Verantwortliche ist für das Dokumentieren jeder Kommunikation mit jeglicher interessierten Partei verantwortlich.

4. Verfahren für Notfälle

4.1. Behandlung eines Notfalls

4.1.1. Pflicht jedes Mitarbeiters zur Meldung von Notfällen

Jeder Mitarbeiter ist verpflichtet, Notfälle wie folgt zu melden:

- [illegible]
- [illegible]

Jedes andere Ereignis oder Systemschwachstellen die sich noch nicht zu einem Notfall entwickelt haben, müssen auf dieselbe Art und Weise gemeldet werden.

Commented [27A13]: Dies muss die im Plan für betriebliches Kontinuitäts-management genannte Person sein.

Commented [27A14]: Hier alle Notfälle aufnehmen, die [illegible]

Commented [27A15]: Falls die Art des Notfalls keine sofortige Behebung erfordert, können diese per E-Mail oder über ein Software-Werkzeug gemeldet werden.

Commented [27A16]: Z.B.: Leiter der IT-Abteilung

Commented [27A17]: Z.B.: Beauftragter für operative Tätigkeiten

Commented [27A18]: Falls dieser Punkt bereits durch das Verfahren zum Umgang mit Informationssicherheitsvorfällen entsprechend ISO 27001 geregelt ist, diesen Text löschen und einen Verweis auf das Verfahren einfügen.

die erste verfügbare Person [Telefonnummer] anrufen und hierüber den Verantwortlichen in seiner/ihrer Organisationseinheit oder den Krisenmanager in Kenntnis setzen.

4.1.2. Notfallbehandlung

Die Person, die eine Information über den Notfall erhält, muss bewerten ob der Notfall/mögliche

- Es muss damit begonnen werden, den Notfall einzugrenzen und zu beheben, wie dies in den folgenden Abschnitten dieses Dokuments beschrieben wird
- alle Verantwortlichen müssen über den Eintritt des Notfalls in ihrem Verantwortungsbereich benachrichtigt werden
-
-

den Krisenmanager informieren. Die an den Krisenmanager weitergegebene Information muss Angaben über die Art und das Ausmaß eines Notfalls sowie seine mögliche Auswirkung beinhalten.

4.1.3. Krisenmanager

Der Krisenmanager muss den Fortschritt bei der Behandlung eines Notfalls und die Unterbrechungsdauer einzelner Aktivitäten überwachen, sowie eine Einschätzung der für die Behebung des Notfalls benötigten Zeitspanne vornehmen.

4.2. Eindämmung und Behebung eines Notfalls

4.2.1. Räumung des Gebäudes (ungeachtet der Art des Notfalls)

Commented [27A19]: Z.B. Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager usw.

Commented [27A20]: Dieses Kapitel liefert nur für einige potentielle Notfälle Vorgehensweisen – das Vorgehen bei anderen Notfällen, die in der Risikoeinschätzung als wahrscheinlich eingestuft wurden, sollte hier hinzugefügt werden.

Für die Räumung des Gebäudes werden die Sammelpunkte genutzt, die in der Liste der Kontinuitäts-Standorte im Anhang des Plans für betriebliches Kontinuitätsmanagement spezifiziert sind.

Krisenmanager	• Falls Gesundheit oder Leben von Menschen bedroht sind, die Anweisung zur Evakuierung geben • [illegible] • [illegible]
Für die Evakuierung verantwortliches Team	• Lenkung der Evakuierung zum Sammelpunkt • [illegible] • [illegible]
Alle Mitarbeiter	• Verlassen des Gebäudes wie im Evakuierungsplan für Ihr Gebäude vorgegeben • Befolgen der Anweisungen des Evakuierungs-Verantwortlichen • [illegible] • [illegible] • [illegible]
[illegible]	• Nachdem sich die Personen am Sammelpunkt eingefunden haben, eine Aufstellung der Anwesenden und Vermissten erstellen

4.2.2. Feuer

Das Gebäude wird gemäß Evakuierungsplan für das Gebäude geräumt.

Krisenmanager	• Falls das Leben oder die Gesundheit von Menschen in Gefahr ist, gibt der Krisenmanager die Anweisung zur Evakuierung • [illegible]

4.2.3. Unterbrechung der Energieversorgung

Krisenstab Support-Team	• Feststellung der Ursache für die Unterbrechung – liegt der Grund bei den Leitungen oder beim Energieversorger
[illegible]	• [illegible]

Commented [27A21]: Z.B. Anlagenanalyst, Anlagentechniker usw.

Alle Mitarbeiter	• [illegible]
[illegible]	• Überwachung von USV-Geräten und gegebenenfalls Herunterfahren von Informationssystemen

4.2.4. Erdbeben

Das Gebäude wird gemäß Evakuierungsplan für das Gebäude geräumt.

Alle Mitarbeiter	• Schutz unter einem Türrahmen, in der Nähe einer tragenden Wand oder unter einem Tisch suchen • Aufzüge nicht benutzen • [illegible] • [illegible] • [illegible]
[illegible]	• Falls das Leben oder die Gesundheit von Menschen in Gefahr ist, die Evakuierung des Gebäudes anordnen, sobald das Erdbeben vorüber ist
Krisenstab Support-Team	• [illegible] • [illegible]

4.2.5. Drohbrief

Alle Mitarbeiter	• Falls sie einen verdächtigen Brief erhalten, öffnen Sie diesen nicht und berühren Sie ihn nur an den äußeren Kanten • [illegible] • [illegible] • [illegible]
[illegible]	• Benachrichtigen Sie die Polizei unter [Telefonnummer] • [illegible] • [illegible]

Commented [27A22]: Z.B.: Sicherheitsbeauftragter

Commented [27A23]: Z.B.: Sicherheitsbeauftragter

Commented [27A24]: Z.B.: Sicherheitsbeauftragter

4.2.6. Drohanruf / Bombendrohung

Alle Mitarbeiter	• Falls Sie einen Drohanruf erhalten, notieren Sie die exakte Zeit und die Telefonnummer des Anrufers • [illegible] • Gestatten Sie es dem Anrufer, möglichst viel ohne Unterbrechung zu reden: - [illegible] - [illegible]

	- Falls Ihr Telefon mit einem Lautsprecher ausgestattet ist, schalten Sie das Telefon auf Freisprechen und bitten Sie jemanden, Notizen zu machen - Wiederholen Sie jede Forderung des Anrufers • Falls es sich um eine Bombendrohung handelt, fragen Sie den Anrufer folgendes: - Wird die Bombe explodieren? Wann ? - Kann sie entschärft werden? Wie ? - [illegible] - [illegible] - [illegible] - [illegible] • Bürotüren nur öffnen, wenn Sie sicher sind, dass diese nicht mit der Bombe verbunden sind • [illegible] • [illegible] • [illegible]
Krisenmanager	• Benachrichtigen Sie den Verantwortlichen der Organisationseinheit die Ziel der Drohung ist • Benutzen Sie die normalen Sammelpunkte nicht – wählen Sie einen neuen Sammelpunkt • [illegible] • [illegible] • [illegible]

4.2.7. Telekommunikations-Ausfall

Mitarbeiter in [Name der Abteilung]	• Jeder Mitarbeiter wird über den Ausfall informiert • [illegible]
[illegible]	• Benutzung alternativer Kommunikationsmittel

Commented [27A25]: Dies sind Verantwortlichkeiten der [illegible]

4.2.8. Ausfall von Informationssystemen

Mitarbeiter in [Name der Abteilung]	• Jeder Mitarbeiter wird über den Ausfall informiert • [illegible] • [illegible]
Krisenmanager	• [illegible]
[illegible]	• Falls möglich, auf andere Arten zur Ausführung von Aktivitäten übergehen

Commented [27A26]: Dies sind Verantwortlichkeiten der Abteilung für Informationstechnologie (IT). Bitte geben Sie den Begriff an, den Sie für die IT-Abteilung in Ihrem Unternehmen verwenden.

4.2.9. Angriff durch Schadsoftware

Mitarbeiter in [Name der Abteilung]	• Jeder Mitarbeiter wird über den Notfall informiert • Falls es sich um einen unbekannten Typ von Schadcode handelt, sollte [Name der für Informationssicherheit verantwortlichen Organisation] benachrichtigt werden • [illegible] • [illegible] • [illegible] • [illegible]
Alle Mitarbeiter	• Trennen Sie jeglichen infizierten PC physikalisch vom Netzwerk; deaktivieren Sie WLANs, Bluetooth, etc. • [illegible]
Mitarbeiter in [illegible]	• Falls der Rechner noch nicht vom Netzwerk getrennt ist, bewerten Sie ob dies zur Vermeidung weiterer Infektionen geschehen sollte • Deaktivieren Sie alle drahtlosen Verbindungen auf dem Rechner • [illegible] • [illegible] • [illegible]

Commented [27A27]: Dies sind Verantwortlichkeiten der Abteilung für Informationstechnologie (IT). Bitte geben Sie den Begriff an, den Sie für die IT-Abteilung in Ihrem Unternehmen verwenden.

Commented [27A28]: Dies sind Verantwortlichkeiten der Abteilung für Informationstechnologie (IT). Bitte geben Sie den Begriff an, den Sie für die IT-Abteilung in Ihrem Unternehmen verwenden.

Commented [27A29]: Dies sind Verantwortlichkeiten der Abteilung für Informationstechnologie (IT). Bitte geben Sie den Begriff an, den Sie für die IT-Abteilung in Ihrem Unternehmen verwenden.

4.2.10. Verletzung interner oder externer Regeln

[Stellenbezeichnung]	• Vorgehensweise entsprechend der Arbeitsrechtsvorschriften zu [illegible]

5. Verwaltung von Aufzeichnungen zu diesem Dokument

Name der	*Aufbewahrung*	*Verantwortlicher für*	*Maßnahme zum Schutz der*	*Aufbewahrung*

Aufzeichnung	***s-Ort***	[illegible]	***Aufzeichnung***	***s-Dauer***
Verzeichnis der Notfälle	[illegible]	[Stellenbezeichnung]	[illegible]	3 Jahre

Commented [27A30]: Geben Sie die Angaben in dieser Spalte an, die Ihre tatsächlichen Bedürfnisse widerspiegeln.

Commented [27A31]: Z.B. Vorfallmanager, Vorfall- Analyst, der den Vorfallbericht erhalten hat, etc.

Commented [27A32]: Z.B. Vorfallmanager, Sicherheitsbeauftragter usw.

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

6. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Dieses Dokument wird, zusammen mit allen zusätzlichen Unterlagen, wie folgt aufbewahrt:

- [illegible]
- [illegible]

Commented [27A33]: Das Dokument so aufbewahren, dass nur Berechtigte Zugang haben; es ist zu prüfen ob Personen außerhalb der Organisation Zugang benötigen.

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

Commented [27A34]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

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

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A35]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.