

ISMS Notfallhandbuch



Word-Vorlage





Word-Vorschau

Hier werden nur Auszüge dargestellt!
Nach dem Erwerb steht Ihnen selbstverständlich die vollständige Version im offenen Dateiformat zur Verfügung.

2 Ablauf der Notfallbehandlung



3 Notfallmeldung

Alle Mitarbeiter sind verpflichtet sämtliche Ereignisse, die Personen-, Sach- und Umweltschäden im Bereich des Unternehmens verursachen bzw. verursachen könnten, zu melden. Alle Vorkommnisse, die sich nicht unerheblich auf das Unternehmen oder auf die Kundenbeziehungen nachteilig auswirken können, z. B. zu Einschränkungen oder Ausfällen im Leistungsangebot führen oder Imageschäden oder Umsatzverluste hervorrufen können, sind, ggf. nach Rücksprache mit einer Führungskraft, ebenfalls weiter zu melden.



Übersicht

- ▶ Grundlage zur Minimierung von Schäden im Notfall
- ▶ Unterstützung bei der Erstellung eines IT Sicherheitskonzeptes
- ▶ Konkrete Handlungsanweisungen für verschiedene Notfälle

...richtet sämtliche Ereignisse, die Person... Bereich des Unternehmens verursachen bzw. ver... Vorkommnisse, die sich nicht unerheblich auf das Unt... Beziehungen nachteilig auswirken können, z. B. zu Einschränkungen im Leistungsangebot führen oder Imageschäden oder Umsatzverlusten verursachen können, sind, ggf. nach Rücksprache mit einer Führungskraft, ebenfalls zu melden.

Die Weitermeldung aller Vorkommnisse bzw. Störungen im Betriebsablauf erfolgt grundsätzlich an:

| Name | Organisationseinheit | Handynr. | Festnetznr. |
|-----------------|----------------------|--------------|--------------|
| Mustermann, Max | | 0123 456 789 | 0123 456 789 |

Werden Ereignisse auf fachlicher Ebene festgestellt, wird die jeweilige Führungskraft informiert. Besondere Meldewege sind in den nachfolgenden Abschnitten aufgeführt.

3.1 Notrufnummern am Beispiel für Deutschland (z. B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger)

| | |
|----------------|--------------|
| Feuerwehr | 112 |
| Polizei | 110 |
| Notarzt | 19222 |
| Stromversorger | 0123 456 789 |

...ierungsplan und Meldewege

...weisungen zu speziellen Ereignissen sind als Anla... efügt. Hier sind auch jeweils die entsprechen... dewege aufgeführt.





Inhalt

1 Einleitung

1.1 Allgemeines

Das vorliegende Dokument beinhaltet die Behandlung von Notfällen im Unternehmen – insbesondere bezogen auf Vorfälle im Rahmen der Informationssicherheit.

Auf der Grundlage der DIN EN ISO 27001 wurden die auf das Unternehmen bezogenen, möglichen Notfallsituationen ermittelt. Dabei gilt grundsätzlich die folgende Definition:

Notfall ist jede ungeplante und unerwartete Situation, die eine erhebliche Störung der Prozesse und Abläufe verursacht. Zur Aufrechterhaltung der Geschäftstätigkeit wird ein besonderer Einsatz von Ressourcen (z.B. Personal, Kapital, Wissen, etc.) benötigt, der nicht im normalen Ablauf im Unternehmen verfügbar ist. Dabei ist besonders ein unmittelbarer Sicherheitsbezug – wie z. B. eine Gefährdung der körperlichen Unversehrtheit von Mitarbeitern, ein Brand oder eine Überschwemmung – in einer Notfallbehandlung zu berücksichtigen.

Für die Notfallvorsorge und –behandlung sind u. a. folgende Gefährdungslagen zu berücksichtigen:

- Höhere Gewalt
 - Extremwetterlagen (z. B. Hochwasser, Stürme, Dauerschneefall)
 - Erdbeben
 - Blitzschlag
- Technisches Versagen
 - Freisetzung von Gefahrstoffen in Luft, Boden, Wasser
 - Explosionen
 - Brände

Zunächst erhalten Sie allgemeine Hintergrundinformationen zum Notfall.



Inhalt



3 Notfallmeldung

Alle Mitarbeiter sind verpflichtet sämtliche Ereignisse, die Personen-, Sach- und Umweltschäden im Bereich des Unternehmens verursachen bzw. verursachen könnten, zu melden. Alle Vorkommnisse, die sich nicht unerheblich auf das Unternehmen oder auf die Kundenbeziehungen nachteilig auswirken können, z. B. zu Einschränkungen oder Ausfällen im Leistungsangebot führen oder Imageschäden oder Umsatzverluste hervorrufen können, sind, ggf. nach Rücksprache mit einer Führungskraft, ebenfalls weiter zu melden.

Die Weitermeldung aller Vorkommnisse bzw. Störungen im Betriebsablauf erfolgt grundsätzlich an:

| Name | Organisationseinheit | Handynr | Festnetznr |
|-----------------|----------------------|--------------|--------------|
| Mustermann, Max | | 0123 456 789 | 0123 456 789 |

Werden Ereignisse auf fachlicher Ebene festgestellt, wird die jeweilige Führungskraft informiert. Besondere Meldeverfahren sind in den nachfolgenden Abschnitten aufgeführt.

3.1 Notrufnummern am Beispiel für Deutschland (z. B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger)

| | |
|----------------|--------------|
| Feuerwehr | 112 |
| Polizei | 110 |
| Notarzt | 19222 |
| Stromversorger | 0123 456 789 |

.....
.....

Zudem erhalten Sie einen Überblick über den Ablauf im Notfall, die Notfallmeldung und Sofortmaßnahmen.



Inhalt

5.1 Wiederanlauf-Planung

Wiederanlaufpläne und Recoverypläne liegen für die zentralen Server und wichtige Dienste als Anlagen vor.

Durch die IT-Verantwortlichen / Administratoren ist die Klärung folgender Fragen herbeizuführen:

- Welche Komponenten sind nicht mehr brauchbar? (Räume, Netzwerk, Server)
- Was muss neu beschafft werden?
- Was kann bereits in Betrieb genommen werden?
- Fehlen weitere technische/personelle Voraussetzungen?

5.2 Interne / externe Ausweichmöglichkeiten der IT

Es ist zu prüfen, ob und welche Ausweichmöglichkeiten für den Einsatz der IT bestehen:

- in anderes RZ
- in andere naheliegende Geschäftsstelle
- auf andere Server

5.3 Wiederbeschaffungsmöglichkeiten

Die Wiederbeschaffung zu ersetzender, notwendiger Komponenten ist durchzuführen:

- aus eigenen Ressourcen (von anderen Geschäftsstellen, Rechenzentrum)
- über den zentralen Einkauf anhand vorliegende Hardwarebeschreibungen die Minimalanforderungen für das jeweilige System dokumentieren

Die Hardwarebeschreibung sollte folgenden Inhalt haben und jeweils dem Stand der Technik entsprechen: (bereits zum Teil in den Recoveryplänen der einzelnen Maschinen enthalten)

- Bezeichnung, Kaufdatum der IT-Komponente
- Hersteller
- Lieferant und Lieferzeit
- Dauer der Neuinstallation
- Dringlichkeit der Beschaffung
- Herstelleralternativen (um kostengünstig einzukaufen)

5.4 Eingeschränkter IT-Betrieb

Anwendung des Abschaltplans. Hier sind die Komponenten festgelegt, die für einen eingeschränkten IT-Betrieb erforderlich sind.





Inhalt

Der Analysebericht wird der Unternehmensleitung übergeben, insbesondere damit dieser bei etwaigen Rechtsfolgen berücksichtigt werden kann.

6.2 Dokumentation

Alle während der Notfallbehandlung durchgeführten Aktivitäten und Entscheidungen sind revisionssicher zu dokumentieren. Ebenso sind alle an der Notfallbehandlung beteiligten Personen mit ihren jeweiligen Rollen in Listenform zu erfassen.

Die im Rahmen der Notfallbehandlung erforderlichen Dokumente werden regelmäßig aktualisiert und sind so abgelegt, dass sie unverzüglich verwendet werden können.

7 Schulung und Notfallübungen

7.1 Schulung

Alle Mitarbeiter werden bezüglich der Notwendigkeit eines Notfallmanagements regelmäßig sensibilisiert (z. B. durch die Aufnahme des Themas in allgemeinen Teambesprechungen, Informationen in der Mitarbeiterzeitung o. ä.). Schulungen finden insbesondere für Mitarbeiter, die konkret mit den Themen Notfallvorsorge und/oder Notfallbehandlung betraut sind, statt.

Die Führungskräfte unterstützen die Ausbildung und aktive Teilnahme der Mitarbeiter und stellen sie für diese Maßnahmen von ihren alltäglichen Aufgaben frei. Der Nachweis über die durchgeführten Schulungsmaßnahmen wird aufbewahrt.

7.2 Notfallübungen

Durch mindestens jährlich durchgeführte Notfallübungen wird die Vorgehensweise bei

Hilfreiche Erläuterungen und Hinweise helfen Ihnen, in einer Krisensituation den Überblick zu behalten.



Übersicht

Zusätzlich zur Vorlage Notfallhandbuch erhalten Sie jeweils ein Dokument zum konkreten Umgang mit der jeweiligen Krisensituation Bombendrohung, Einbruch, Ausfall Datenübertragungseinrichtung, Ausfall Klimaanlage, Explosion, Stromausfall, Wassereinbruch und Brand.

Bombendrohung per Telefon

Den Anrufer ausführlich reden und wichtige Mitteilungen aufnehmen.

Wenn möglich, Telefongespräch mitschneiden und mithören lassen.

Den Anrufer nicht unterbrechen, nur für die folgenden Fragen:

- Wann wird die Bombe explodieren?
- Wo ist die Bombe?
- Wie sieht sie aus? Was für eine Bombe ist es?
- Was wird die Bombe auslösen?
- Warum machen sie das?
- Wer sind sie? Von wo rufen sie an?

4 Die folgenden Hinweise festhalten:

- Wurde die Nummer angezeigt?
- Wo kam der Anruf her: nah / fern, Handy / Telefon?
- Beschreibung der Stimme: Mann / Frau, jung / alt, hoch / tief?
- Besondere Merkmale der Stimme?
- Gab es Hintergrundgeräusche?

Notieren und interne Weiterleitung entsprechend





Inhalt

I. Eingang der Bombendrohung per Post/Mail

➤ Weiterleitung entsprechend aktuellem Meldeplan

II. Eingang der Bombendrohung per Telefon

- 1 Mit dem Anrufer ausführlich reden und wichtige Mitteilungen aufschreiben
- 2 Wenn möglich, Telefongespräch mitschneiden und mithören lassen
- 3 Den Anrufer nicht unterbrechen, nur für die folgenden Fragen:
 - Wann wird die Bombe explodieren?
 - Wo ist die Bombe?
 - Wie sieht sie aus? Was für eine Bombe ist es?
 - Was wird die Bombe auslösen?
 - Warum machen sie das?
 - Wer sind sie? Von wo rufen sie an?
- 4 Die folgenden Hinweise festhalten:
 - Wurde die Nummer angezeigt?
 - Wo kam der Anruf her: nah / fern, Handy / Telefonzelle?
 - Beschreibung der Stimme: Mann / Frau, jung / alt, Akzent, hoch / tief?
 - Besondere Merkmale der Stimme?

Im Notfall erhalten Sie mit diesen Handlungsanweisungen eine ausführliche Übersicht über das weitere Vorgehen.



Inhalt

Stromausfall im Rechenzentrum, im Bürogebäude sowie in Gebäuden der Geschäftsstellen

(Diese Handlungsanweisung gilt nur für Mitarbeiter der Abteilung zentrale IT)

1 Schadensausmaß ermitteln

a. Bei Stördienst rückfragen.

b. IT Schadensausmaß ermitteln:

- Welche Dienste und Hardware sind betroffen?
- Ist die Klimaanlage betroffen?
- Mitarbeiter informieren entsprechend dem aktuellen Meldeplan.
- Kurzfristiger Ausfall bis 0,5 Std:
 - Maßnahmen für evtl. längerfristigen Ausfall von 0,5 – 8 Std. vorbereiten.
- Längerfristiger Ausfall von 0,5 - 8 Std:
 - alle zentralen Server runterfahren.
 - Maßnahmen für evtl. langfristigen Ausfall ab 8 Std. vorbereiten.
- Langfristiger Ausfall ab 8 Std:
 - alle zentralen Server auf Notstromdiesel legen.
 - Server starten.
 - Funktionstest der unter 1 in Betrieb genommenen Systeme.
 - Mitarbeiter entsprechend dem aktuellen Meldeplan informieren über eingeschränkte Funktionalität

2 Stromversorgung wieder auf normales Netz umstellen

3 Funktionalität aller Dienste prüfen

4 Mitarbeiter informieren entsprechend dem aktuellen Meldeplan



Kostenloser Update-Service

Bei ISO-Revisionsänderungen **innen 1 Jahres** nach Kauf dieses Vorlagenpakets wird Ihnen das Paket inklusive aktueller Normrevision **kostenfrei** zur Verfügung gestellt.





Sofortdownload

Ihr Komplettpaket steht Ihnen nach dem Kauf sofort zur Verfügung.





Zufriedenheitsgarantie

Ihre Autoren - mit **Erfahrung für Sie!**



Aus der **Praxis für Ihre Praxis**. Unsere Vorlagen, Checklisten, Formblätter und Schulungsunterlagen stammen alle von **erfahrenen Beratern**, die diese Musterdokumente mit ihrem ganzen **Erfahrungsschatz** für Sie erstellt haben.