Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungsrahmenwerk Notfallmanagement

Leitlinie - Ausfüllanleitung

Modul Leitlinie

Version 1.0

Februar 2013

Inhaltsverzeichnis

0. Einleitung

Diese Ausfüllanleitung soll bei der Erstellung der Leitlinie zum Notfallmanagement unterstützen. Die Kapitel der Ausfüllanleitung tragen die gleichen Namen wie die Kapitel in der Dokumentenvorlage, um dieses Modul möglichst effizient abarbeiten zu können.

Diese Ausfüllanleitung soll bei der Erstellung der Leitlinie zum Notfallmanagement unterstützen. Die Kapitel der Ausfüllanleitung adressieren inhaltlich die Kapitel in der Dokumentenvorlage und sind dort entsprechend auszuformulieren.

Die in diesem Dokument in *kursiver* Schrift dargestellten Texte sind Beispieltexte, die bei der Erstellung einer Leitlinie verwendet werden können. Die in der Dokumentenvorlage in *kursiver* Schrift dargestellten Texte sind Hinweistexte.

1. Hinweise zum Ausfüllen der Leitlinienvorlage

1.1 Definition des Notfallmanagements

Bei der Formulierung dieses Kapitels ist auf folgende Aspekte einzugehen:

- Was wird von der Institutionsleitung unter Notfallmanagement verstanden?
- Wie definiert die Institutionsleitung die Aufgaben und Kompetenzen der Rollen des Notfallmanagements?
- Welche Schnittstellen (Zuständigkeiten und gegebenenfalls Rechte und Pflichten) gibt es zu anderen Managementsystemen (beispielsweise IT-Management, Informationssicherheitsmanagement, Gebäudemanagement, Qualitätsmanagement oder Risikomanagement)?

Beispieltext:

Die/das/der <Name der Institution> strebt einen kontinuierlichen, unterbrechungsfreien Geschäftsbetrieb beziehungsweise eine unterbrechungsfreie Aufgabenerfüllung an. Um dieses Ziel zu erreichen, wurde von der Leitung der <Name der Institution> entschieden, ein angemessenes Notfallmanagement zu etablieren.

Das Notfallmanagement des/der <Name der Institution> richtet sich nach dem Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 100-4 Notfallmanagement aus. Es ist durch den Baustein B 1.3 "Notfallmanagement" der IT-Grundschutz-Kataloge in das Informationssicherheitsmanagement eingebunden.

Das Notfallmanagement wird alle für den Geschäftsbetrieb oder für die Aufgabenerfüllung kritischen Prozesse mit entsprechenden Notfallvorsorgemaßnahmen und/oder Notfallplänen absichern.

Um alle Belange des Notfallmanagements zu betreuen, wurde die Rolle eines Notfallbeauftragten eingerichtet. Im/In der <Name der Institution> ist dies <Name der Notfallbeauftragten>, sein/ihr Stellvertreter ist <Name des Stellvertreters>.

Bei Bedarf werden für Teilaufgaben des Notfallmanagements weitere Mitarbeiterinnen und Mitarbeiter hinzugezogen. Die personelle Besetzung dieser Teams wird aufgabenbezogen festgelegt.

Der/die/das <Name der Institution> ist bestrebt, solche Aktivitäten zu vermeiden, die ein unvertretbares Risiko bedeuten.

1.2 Stellenwert und Zielsetzung

Hier ist zu beschreiben, warum ein Notfallmanagement für die Institution erforderlich und wichtig ist und auch, warum die Institutionsleitung für ein funktionierendes Notfallmanagement erforderlich ist.

Es sind die Ziele zu beschreiben, welche von der Institutionsleitung durch die Einführung eines Notfallmanagements verfolgt werden. Hierfür sind folgende Punkte zu beachten:

- Welche verschiedenen Zeithorizonte (kurzfristig, mittelfristig, langfristig) für die Umsetzung der verschiedenen Aufgaben zur Etablierung bzw. Betrieb eines Notfallmanagements gibt es in der Institution?
- Welche Geschäftsziele oder Fachaufgaben sollen durch das Notfallmanagement geschützt werden?
- Gibt es geschäftliche Ziele oder Aufgaben der Institution, die explizit ein Notfallmanagement erfordern?
- Welche wichtigen internen und externen Interessengruppen gibt es, die ein Interesse am Notfallmanagement der Institution äußern könnten (Eigeninteresse oder um die Interessen Dritter wie der Öffentlichkeit zu wahren) und Einfluss auf das Notfallmanagement haben können? Mögliche Interessengruppen wären z. B. Mitarbeiter und deren Angehörige, Kunden (Bürger), Dienstleister, Aufsichtsbehörden oder auch der Gesetzgeber.

Beispieltexte:

Um die Geschäftsziele des/der <Name der Institution> zu erreichen / Damit die Behörde <Name der Institution> ihre Aufgaben erfüllen kann, werden Ressourcen wie Personal, Informationen, Infrastruktur und Dienstleister benötigt. Falls aufgrund eines Vorfalls die benötigten Ressourcen nicht mehr zur Verfügung stehen, kann der Geschäftsablauf beziehungsweise die Aufgabenerfüllung gefährdet werden.

Unsere Mitarbeiter, Partner und Kunden (Bürger) erwarten jedoch, dass eine hinreichend qualifizierte Vorsorge für alle relevanten Szenarien getroffen wird und dass ein eingetretener

Schaden schnell, systematisch und adäquat begrenzt und behoben werden kann. Um diesen Erwartungen gerecht zu werden, benötigt der/die/das <Name der Institution> ein effektives und effizientes Notfallmanagement und setzt diesen ganzheitlichen Managementprozess um.

Der/die/das <Name der Institution> nutzt das Notfallmanagement, um den Geschäftsbetrieb beziehungsweise die Aufgabenerfüllung auch bei einem Ausfall wesentlicher Ressourcen aufrechterhalten zu können und Notfälle und Krisen beherrschbar zu machen. Der/die/das <Name der Institution> verfolgt damit die folgenden Ziele:

- *<Bitte Ziele formulieren>*
- *Der Schutz von Mitarbeitern muss auch in Notfällen jederzeit sichergestellt sein.*
- *Die Institution gewährleistet, dass die Aufgaben des/r <Name der Institution> und die Dienstleistungen gegenüber (nachgeordneten) Institutionen sowie den Kunden/Bürgern erfüllt und kontinuierlich ausgeführt werden können.*
- *Das positive Image des/der <Name der Institution> darf in der Öffentlichkeit nicht durch fehlende Notfallvorsorge beeinträchtigt werden.*
- *Die Zusammenarbeit mit Dienstleistern/Lieferanten muss bei kritischen Geschäftsprozessen und Aufgaben auch in Notfällen mit geeigneten Notfallvorkehrungen aufrechterhalten werden können.*

1.3 Kernaussagen der Notfallstrategie

Hier sind die strategischen Ziele festzulegen, die mit dem Aufbau und dem Betrieb des Notfallmanagements verfolgt werden:

- Was ist das primäre Ziel bei der Notfallbehandlung?
- Welche Arten von Geschäftsunterbrechungen beziehungsweise Unterbrechung der Aufgabenerfüllung werden als kritisch angesehen?
- Welche Schadensszenarien sind ausschlaggebend?
- Welche Bereitschaft besteht, Risiken einzugehen, beziehungsweise wie hoch ist das Risikoakzeptanzniveau?
- In welcher Art und Größenordnung soll etwas gegen diese Risiken unternommen werden?

Beispieltext:

Das Notfallmanagement berücksichtigt gleichermaßen präventive Komponenten (Notfallvorsorge) als auch reaktive Komponenten (Notfallbewältigung). Auf diese Weise versetzt das Notfallmanagement der/die/das <Name der Institution> in die Lage, bei Notfällen und Krisen, ihre Geschäftstätigkeit beziehungsweise Aufgabenerfüllung, wenn auch im Rahmen eines Notbetriebes leistungsreduziert, aufrechtzuerhalten. Dies ist insbesondere bei solchen wichtig, in denen ganze Personengruppen oder weite Teile der Infrastruktur betroffen sind.

Die zentralen Ziele des Notfallmanagements sind hierbei:

- *die Widerstandsfähigkeit von Geschäftsprozessen gegen störende Einflüsse zu erhöhen*
- *die Fortführung von kritischen Geschäftsprozessen im Notbetrieb zu gewährleisten*

Hierzu werden die Geschäftsprozesse analysiert, nach ihrer Kritikalität eingestuft und die jeweils unterstützenden Ressourcen betrachtet. Die kritischen Geschäftsprozesse und deren Abhängigkeiten zu unterstützenden Ressourcen zu erkennen, stellt die Basis für ein wirkungsvolles Notfallmanagement dar.

Auch ohne dass konkret ein Schadensereignis eingetreten ist, müssen Vorkehrungen gegen deren Auswirkungen getroffen werden, um in Notfällen schnell und erfolgreich handeln zu können. Dazu gehört auch, dass mögliche Ursachen von Schadensereignissen beziehungsweise Schwachstellen beseitigt werden.

Der/die/das <Name der Institution> betrachtet im Notfallmanagement die folgenden wesentlichen Szenarien:

- *<Szenarien anpassen>*
- *Ausfall des primären Rechenzentrums*
- *Ausfall des Verwaltungsstandorts Berlin, Musterstraße 12*

Eine entsprechende detaillierte Analyse der Auswirkungen, die durch diese Ausfallszenarien hervorgerufen werden können, wird innerhalb des Notfallmanagements durchgeführt.

Das Notfallmanagement wird unter den folgenden Randbedingungen betrieben:

- *<Bitte Randbedingungen formulieren>*
- *Primäres Ziel bei der Notfallbehandlung ist es, die Ausweitung eines Schadens zu minimieren.*
- *Es wird geprüft, für welche Notfälle Notfalldienstleister mit eingeplant werden.*

1.4 Festlegung des Geltungsbereichs

Der Geltungsbereich des Notfallmanagements der Institution ist eindeutig festzulegen. Der Geltungsbereich sollte in sich abgeschlossen und nicht zu eng gefasst sein. Es sind folgende Rahmenparameter bei der Definition des Geltungsbereichs zu beachten:

- Welche Standorte sollen betrachtet werden (alle Standorte, einzelne Standorte oder in Ausnahmefällen nur Teilbereiche)?
- Welche nachgeordneten Institutionen werden betrachtet?
- Welche Geschäftsbereiche sollen betrachtet werden?
- Welche Geschäftsprozesse beziehungsweise Fachaufgaben sind mit einzubeziehen?
- Sind alle relevanten Ressourcen erfasst?
- Sind alle unterstützenden Prozesse erfasst?

Eine Beschreibung des Geltungsbereichs sollte eventuell vorgenommene Einschränkungen und Grenzen des Notfallmanagements enthalten. Optional können die wesentlichen Geschäftsprozesse beziehungsweise Fachaufgaben innerhalb des Geltungsbereichs hervorgehoben werden.

Beispieltext:

Die Festlegungen dieser Leitlinie gelten für der/die/das gesamte <Name der Institution>. Bei den Detailplanungen zur Ausgestaltung des Notfallmanagements werden daher alle Standorte und Abteilungen einbezogen. Außerdem wurden zusätzlich die folgenden Bereiche/Institutionen eingebunden: (z. B. nachgeordnete Institutionen).

Die Leitlinie zum Notfallmanagement gilt sowohl für interne und externe Mitarbeiter und ist auch für die Einbindung von Dienstleistern, wie beispielsweise IT-Dienstleistern, bindend.

Jegliche Ausnahmen von Notfallplänen und –vorkehrungen sind zu begründen und zu dokumentieren. Außerdem bedürfen sie der expliziten Zustimmung durch den Notfallbeauftragten.

1.5 Regulatorische Anforderungen und sonstige Vorgaben

Es gibt eine Vielzahl unterschiedlicher regulatorischer Anforderungen und sonstigen Vorgaben für Institutionen, je nach Art und Branche. Daher muss jede Institution alle relevanten Gesetze, Verordnungen, Erlasse, Satzungen, Geschäftsordnungen, Richtlinien und Vorschriften identifizieren, die für das Notfallmanagement von Bedeutung sind.

Rechtliche Anforderungen zum Notfallmanagement ergeben sich beispielsweise aus dem

- Umsetzungsplan Bund – Gewährleistung der IT-Sicherheit in der Bundesverwaltung,
- Umsetzungsplan KRITIS – Schutz Kritischer Infrastrukturen,
- dem Arbeitsschutzgesetz (ArbSchG) und
- der Betriebssicherheitsverordnung (BetrSichV).

Die jeweiligen rechtlichen Anforderungen zum Notfallmanagement sind geeignet zu dokumentieren.

Beispieltext:

Die für den/die/das <Name der Institution> maßgeblichen juristischen Anforderungen zum Notfallmanagement werden nachfolgend aufgelistet und in die im Folgenden aufgeführten Bereiche unterteilt.

- *Gesetze*
  - <...>
- *Verordnungen*
  - <...>
- *Erlasse*
  - <...>
- *Satzungen*

    - <...>
- *Verträge*
    - <...>
- *Geschäftsordnungen*
    - <...>
- *Allgemeine Richtlinien und Standards*
    - *UP Bund*
    - *UP KRITIS*
    - *BSI-Standard 100-4*
    - **<...>**

1.6 Notfallorganisation, Rollen und Verantwortlichkeiten

Hier sind

- der Aufbau der Notfallorganisation,
- die wichtigsten Rollen (Prävention und Reaktion) und ihre Verantwortlichkeiten in Kurzform

zu beschreiben.

Mögliche Rollen in der Prävention können sein:

- Institutionsleitung
- Notfallbeauftragter
- Notfallkoordinatoren
- Notfallvorsorgeteam

Mögliche Rollen in der Reaktion können sein:

- Krisenentscheidungsgremium
- Krisenstab
- Leiter und Kernteam des Krisenstabs
- Erweiterter Krisenstab
- Fachberater im Krisenstab
- Notfallteams
- Unterstützendes Zusatzpersonal

Eine ausführliche Beschreibung der Rollen und der Notfallorganisation ist im Modul Notfallvorsorgekonzept enthalten.

Alle Rollen sollten bereits an dieser Stelle mit konkreten Namen und Telefonnummern (z. B.: Notfallbeauftragter: Herr Mayer -1234) oder aber mindestens mit konkreten Positionsbeschreibungen (Notfallbeauftragter: Referatsleiter Innerer Dienst) versehen werden.

Beispieltext:

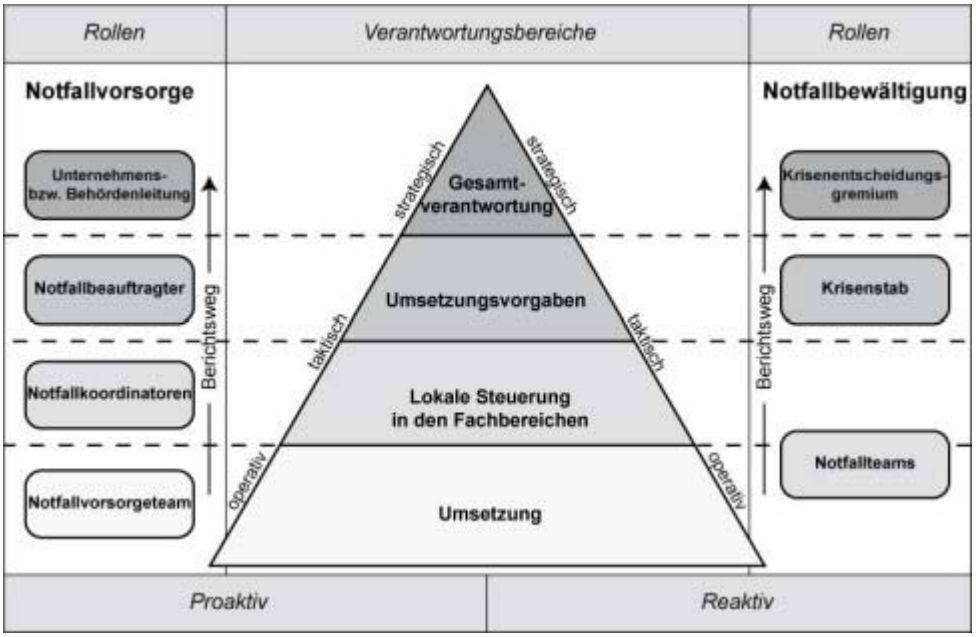

Abbildung 1: Rollen und Verantwortungsbereiche

*Die **Institutionsleitung** ist für die institutionsweite Sicherstellung des Notfallmanagements verantwortlich. Sie legt die Bedeutung des Notfallmanagements in der Institution fest, bestimmt die strategische Ausrichtung bei der Etablierung und stellt die notwendigen finanziellen und personellen Ressourcen nach wirtschaftlichen Ansätzen zur Verfügung.*

*Der **Notfallbeauftragte** steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit. Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente und Regelungen zuständig.*

Der Notfallbeauftragte wird von der Leitung der Institution ernannt und mit den erforderlichen Kompetenzen ausgestattet.

*Der **Krisenstab** ist ein planendes, koordinierendes, informierendes, beratendes und unterstützendes Gremium. Er stellt eine besondere temporäre Aufbauorganisation dar, die die normale Aufbauorganisation für die Bewältigung eines Notfalls auflöst und Organisationseinheiten-übergreifende Kompetenzen bündelt.*

Die weiteren Rollen der Notfallorganisation und deren Verantwortungsbereiche werden im Notfallvorsorgekonzept ausführlich beschrieben.

1.7 Kontinuierliche Verbesserung

Das Notfallmanagement ist ein kontinuierlicher Prozess, der zyklisch auf Optimierungsbedarf überprüft werden muss. Hierfür sind regelmäßige Überprüfungen (beispielsweise durch die interne Revision) sowie Tests und Übungen durchzuführen.

Es ist anzugeben, durch welche konkreten Schritte der Notfallmanagement-Prozess kontinuierlich verbessert werden soll. Dazu ist es nötig, Aussagen über die Überprüfungsintervalle zu machen. Zudem ist die Art der Überprüfung zu benennen und es ist festzulegen, wer die Überprüfung steuert.

Beispieltext:

Die Effektivität und Effizienz des Notfallmanagements und der umgesetzten Vorsorgemaßnahmen werden <Bitte Periode angeben> bewertet. Hierfür werden regelmäßig Überprüfungen sowie Tests und Übungen durchgeführt.

Da durch Tests und Übungen in der Regel nur einzelne Bestandteile des Notfallmanagements überprüft werden, sollen für die kontinuierliche Verbesserung des Notfallmanagements zusätzlich alle <Zeitdauer angeben> interne / externe Audits durchgeführt werden.

Durch Tests und Übungen sollen Leistungsfähigkeit und Wirksamkeit des Notfallmanagements in möglichst vielen Organisationseinheiten und Geschäftsprozesse untersucht werden. Die jeweils einbezogenen Organisationseinheiten werden rechtzeitig darüber informiert und unterstützen das Notfallmanagement aktiv bei der Durchführung der Tests und Übungen.

Der Prozess zur kontinuierlichen Verbesserung des Notfallmanagements wird vom <Rolle eintragen; für gewöhnlich der Notfallbeauftragte> gesteuert und durch <Rolle eintragen> die Ergebnisse an die Leitungsebene berichtet.

1.8 Überwachung der Umsetzung

Dieses Kapitel ist optional.

Es ist zu beschreiben, wie und durch wen in der Institution die Umsetzung der Vorgaben der Leitlinie zum Notfallmanagement überwacht wird. Des Weiteren ist zu beschreiben, wie und an wen Abweichungen von der Leitlinie gemeldet und nach welchen Kriterien diese Meldungen geprüft werden. Auch die angemessene Reaktion auf festgestellte Abweichungen muss beschreiben werden.

Beispieltext:

Die Umsetzung der Vorgaben der Leitlinie zum Notfallmanagement wird vom Notfallbeauftragten überwacht. Abweichungen von dieser Leitlinie oder sich daran anschließende Regelwerke werden an den Notfallbeauftragten gemeldet, geprüft und gegebenenfalls im Rahmen der geltenden Berichtswege eskaliert.

1.9 Freigabe und Aktualisierung der Leitlinie

Die Leitlinie muss allen Mitarbeitern und Interessengruppen sowie Prozessbeteiligten nach der Freigabe durch die Leitung der Institution bekannt gegeben werden. Deshalb sind die berechtigten Rollen im Verteilerkreis (innerhalb der Dokumenteninformationen) anzugeben. Es ist ein Aktualisierungszyklus (beispielsweise jährlich) anzugeben.