

---

## Erstellung eines Notfallplanes (Erfahrungsbericht)

---



**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

---

Wilfried Gericke  
Dr.Phil(USA) Dipl.-Math.  
Sicherheitsbevollmächtigter  
IT-Sicherheitsbeauftragter

---

Erstellung Notfallplan

---

**Motivation**

**begriffliche Grundlagen**

**juristischer Blickwinkel**

**Werkzeuge**

**Randbedingungen für das INT**

**Erfahrungsbericht**

---

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

## Erstellung Notfallplan

**Motivation****Seminar für Sicherheitsbevollmächte (Geheimchutz für die Wirtschaft)**

„wir gehen natürlich davon aus, dass Sie einen Notfall/Katastrophenplan haben“

**Frühjahrsseminar der IT-Sicherheitsbeauftragten der FhG****Aktualisierung der Anweisungen an den Wachdienst (Erneuerung der Zertifizierung)**

Seite 3

Rheinlandtreffen 12.11.2008

## Erstellung Notfallplan

## begriffliche Grundlagen

**Kontinuitätsmanagement**

Betriebliches **Kontinuitätsmanagement** bezeichnet in der Betriebswirtschaftlehre Konzepte, Planungen und Maßnahmen zur Aufrechterhaltung der betrieblichen Kontinuität, abgekürzt auch als **BKM**.

Herleitung aus dem (engl.) *business continuity management (BCM)*.

Das BKM bezeichnet zusammenfassend eine Managementmethode, die anhand eines Lebenszyklus-Modells die Fortführung der Geschäftstätigkeit unter Krisenbedingungen oder zumindest unvorhersehbar erschwerten Bedingungen absichert. Es besteht eine enge Verwandtschaft mit dem Risikomanagement.

In den deutschsprachigen Ländern wird das BKM bisweilen als verwandt mit der Informationssicherheit, der IT-Notfallplanung und dem Facilities Management angesehen.

Verbindungen bestehen auch zum Gedankengut der Corporate Governance.

Seite 4

Rheinlandtreffen 12.11.2008

---

Erstellung Notfallplan

---

begriffliche Grundlagen

**Kontinuitätsmanagement**

Methode und Rahmen des BKM sind im sog. "Good Practice Guide" veröffentlicht, der durch das (GB) Business Continuity Institute herausgegeben wird.  
Zentrale Kompetenzen für Praktiker sind in den (GB, USA) "Joint Standards" geregelt, die gemeinsam durch das Business Continuity Institute und das Disaster Recovery Institute International herausgegeben werden.

Das BSI hat gerade den neuen Standard BSI 100-4 "Notfallmanagement" fertig gestellt, der als Ergänzung zum IT-Grundschutz das Thema BKM darstellt.

---

Seite 5

Rheinlandtreffen 12.11.2008

---

Erstellung Notfallplan

---

begriffliche Grundlagen

**Kontinuitätsmanagement**

Ziel des Business Continuity-Management ist die Generierung von Prozessdefinitionen und Dokumentation eines betriebsbereiten und dokumentierten **Notfallvorsorge-Plans**, der exakt auf das individuelle Unternehmen abgestimmt ist, sowie die Sensibilisierung aller Mitarbeiter auf das Thema

"wirtschaftliche Existenzsicherung bei einer unternehmenskritischen Notfallsituation".

---

Seite 6

Rheinlandtreffen 12.11.2008

"Es kommt nicht darauf an, die Zukunft vorauszusehen, sondern auf die Zukunft vorbereitet zu sein."

*Perikles, griech. Staatsmann, 493-429 v. Chr.*

begriffliche Grundlagen

**Kontinuitätsmanagement**

Seit November 2007 existiert ein zertifizierbarer Standard zum Business Continuity Management (BCM), der BS 25999. Dieser besteht aus zwei Teilen:  
dem Leitfaden (code of practice), der bereits im November 2006 erstellt wurde sowie  
zertifizierbare Spezifikationen.

## Erstellung Notfallplan

begriffliche Grundlagen

**Notfallplan****Was ist ein Notfall?**

Ein **Notfall** ist ein unerwünschtes, zeitlich nicht vorhersehbares Ereignis, dessen Eintritt nach menschlichem Ermessen sehr wahrscheinlich ist.

**Was ist ein Notfallplan?**

Ein Notfallplan ist ein Werkzeug, mit dem ein Unternehmen auf plötzlich eintretende Notfälle, verursacht durch Feuer, Unglücksfälle, Betriebsstörungen usw. schnell und angemessen reagieren kann.

Zur Bewältigung des Notfalles benötigt man organisatorische Unterstützung, weil die Struktur des Unternehmens üblicherweise nicht darauf abgestimmt ist. Ein Notfallplan bietet organisatorische Hilfe bei der Abwicklung außerplanmäßiger Ereignisse. Er beinhaltet Alarmierungschecklisten, Maßnahmenblätter, Kommunikationswege und technische Details.

Seite 9

Rheinlandtreffen 12.11.2008

## Erstellung Notfallplan

begriffliche Grundlagen

**Notfallplan****Warum ist ein Notfallplan erforderlich?**

Der Unternehmer bzw. die von ihm beauftragten Personen tragen die Organisationsverantwortung im Unternehmen. Sie sind persönlich verantwortlich für schnelle und richtige Entscheidungen bei Not- und Unglücksfällen.

Ein funktionsfähiger Notfallplan stellt eine wichtige Entscheidungshilfe in Krisensituationen dar.

Seite 10

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

begriffliche Grundlagen

**Notfallplan**

**Organisationsverschulden**

Unter **Organisationsverschulden** versteht man die schuldhafte Verletzung von Organisationspflichten oder das Nichterfüllen rechtlicher Anforderungen an betriebliche, organisatorische Maßnahmen. Dabei bezieht sich der Begriff »Organisation« sowohl auf die Abläufe in einem Unternehmen wie auf das Unternehmen selbst.

Im Schadensfall wird einem Unternehmen ein Organisationsverschulden zur Last gelegt, wenn es nicht nachweisen kann, dass alle zur Schadensvermeidung vorgeschriebenen bzw. erforderlichen Maßnahmen eingehalten bzw. ergriffen wurden.

Neben der Haftung der Organisation im Ganzen prüfen die Gerichte auch das Verschulden einzelner Beteiligter.

Aus der Rechtsprechung ergibt sich, dass ein Unternehmen für die Kontrolle sämtlicher betrieblicher Abläufe verantwortlich ist. Dabei sind auch die Folgen einzelner Handlungen auf ihre Rechtsverträglichkeit zu überprüfen.

Seite 11

Rheinlandtreffen 12.11.2008


  
**Fraunhofer** Institut
   
 Naturwissenschaftlich-Technische Trendanalysen

Erstellung Notfallplan

---

begriffliche Grundlagen

**Notfallplan**

**Versuchen Sie, die aufgeführten Fragen zu beantworten:**

Gibt es in Ihrem Betrieb einen Notfallplan?  
 Wissen Sie auf Anhieb wo der Plan liegt, bzw. wie Sie an die Daten kommen?  
 Wird der Plan regelmäßig auf Aktualität überprüft?  
 Ist der Zugriff auf den aktuellen Plan zu jeder Zeit für alle Verantwortlichen möglich?  
 Gibt es in Ihrem Unternehmen Personal, welches auf Sicherheitsfragen spezialisiert ist?  
 Ist der Aufwand für die Erstellung, Pflege und Fortführung nebenbei zu erledigen?  
 Ist der Plan durch Fachleute geprüft worden?  
 Haben Sie den Plan praktisch auf Durchführbarkeit überprüft?  
 Führen Sie im Unternehmen regelmäßig Notfallübungen durch?

Quelle: [www.notfallplan.net](http://www.notfallplan.net)

Seite 12

Rheinlandtreffen 12.11.2008


  
**Fraunhofer** Institut
   
 Naturwissenschaftlich-Technische Trendanalysen

Erstellung Notfallplan

---

Werkzeuge:

Voruntersuchung:

- Notfallszenarien
- Annahmen
- Wirkungsszenarien
- Verantwortung
- Einbindung Externer
- Mgmt-System
- Notfallbehandlung


Planerstellung:

- Notfallpläne
- Anforderungen
- Testszenarien
- Testplan
- Fortführung

Empfehlung von Dr.Dirk Loomans von Loomans&Matz AG

---

Seite 13  
Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---


**BSI-Standards**

BSI-Standards enthalten Empfehlungen des BSI zu  
Methoden,  
Prozessen und  
Verfahren sowie  
Vorgehensweisen und  
Maßnahmen

mit Bezug zur Informationssicherheit.

---

Seite 14  
Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---

### BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

Der vorliegende BSI-Standard definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der anderen ISO-Standards der ISO 2700x-Familie wie beispielsweise ISO 27002 (früher ISO 17799). Er bietet Lesern eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktischere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie zur IT-Grundschutz-Vorgehensweise kompatibel ist.

Seite 15

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

### BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrecht erhalten und verbessert werden kann, wird beantwortet.

IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards der 2700x-Reihe und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundinformationen und Beispielen. Im Zusammenspiel mit den IT-Grundschutz-Katalogen wird in der IT-Grundschutz-Vorgehensweise nicht nur erklärt, was gemacht werden sollte, sondern es werden auch konkrete Hinweise gegeben, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Standards nachzukommen.

Seite 16

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

### **BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz**

Die IT-Grundschutz-Kataloge des BSI enthalten Standard-Sicherheitsmaßnahmen aus den Bereichen Organisation, Personal, Infrastruktur und Technik, die bei normalen Sicherheitsanforderungen in der Regel angemessen und ausreichend zur Absicherung von typischen Geschäftsprozessen und Informationsverbänden sind. Viele Anwender, die bereits erfolgreich mit dem IT-Grundschutz-Ansatz arbeiten, stehen vor der Frage, wie sie mit Bereichen umgehen sollen, deren Sicherheitsanforderungen deutlich über das normale Maß hinausgehen. Wichtig ist dabei, dass die zugrundeliegende Methodik möglichst wenig zusätzlichen Aufwand mit sich bringt und möglichst viele Ergebnisse aus der IT-Grundschutz-Vorgehensweise wiederverwendet. Vor diesem Hintergrund hat das BSI einen Standard zur Risikoanalyse auf der Basis von IT-Grundschutz erarbeitet.

Diese Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit den IT-Grundschutz-Maßnahmen arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten.

---

Seite 17

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

### **BSI-Standard 100-4 Notfall-Management**

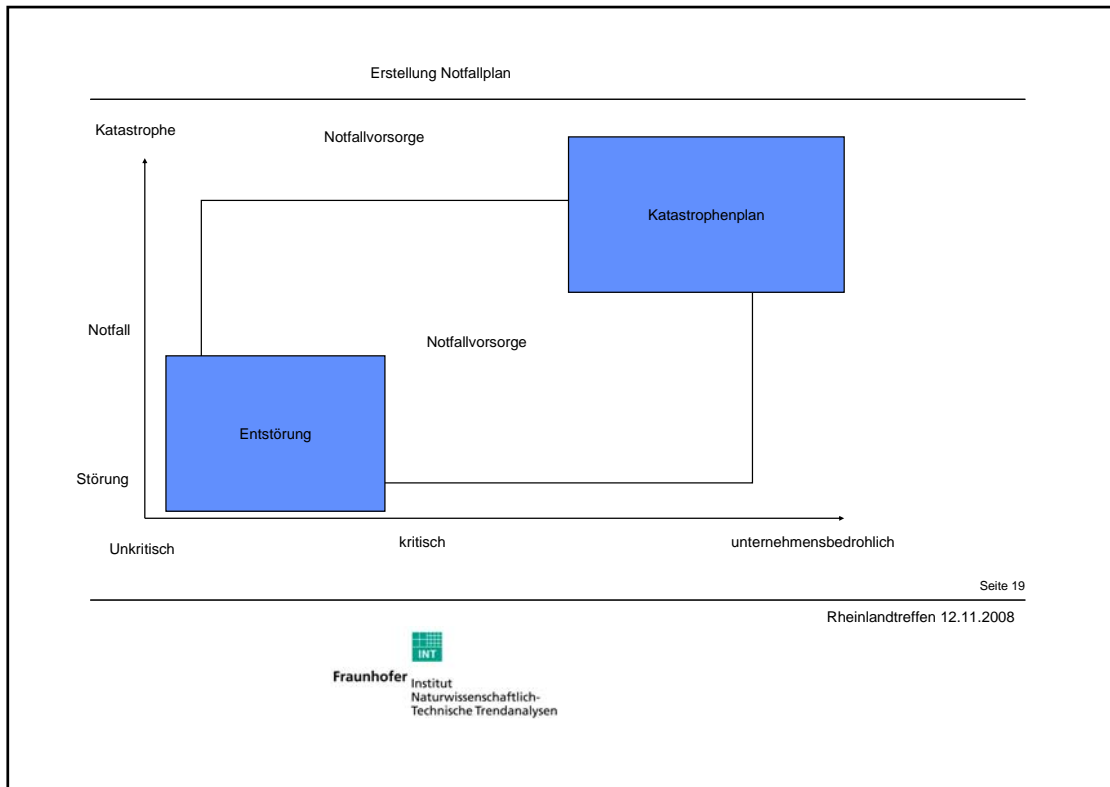
Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, um bei Notfällen der verschiedensten Art adäquat und effizient reagieren und die wichtigen Geschäftsprozesse schnell wieder aufnehmen zu können.

Details hierzu im separaten Vortrag heute Nachmittag

---

Seite 18

Rheinlandtreffen 12.11.2008



- Erstellung Notfallplan
- Notfallvorsorge
- Maßnahmenkatalog Notfallvorsorge nach BSI
- Notfallplan erstellen
  - Definition Notfall je nach System
  - Hoher Schaden möglich (Betriebsausfall, finanzielles Desaster, Imageverlust)
  - Meldewege/Adressen/Ansprechpartner festlegen
  - Verfahren festlegen
  - Verantwortliche festlegen
  - Befugnis zur Entscheidung
  - Wiederanlaufplan
  - Notfallübungen
  - Rufbereitschaft
- Seite 20  
Rheinlandtreffen 12.11.2008
-   
**Fraunhofer** Institut  
 Naturwissenschaftlich-  
 Technische Trendanalysen

---

Erstellung Notfallplan

---

Notfallplan

Kosten

Um eine unter Wirtschaftlichkeitsgesichtspunkten angemessene Notfallvorsorge betreiben zu können, müssen die entstehenden Kosten dem potentiellen Schaden (Kosten aufgrund mangelnder Verfügbarkeit im Notfall) gegenübergestellt und bewertet werden. Als Kosten sind zu betrachten:

Kosten für die Erstellung eines Notfallvorsorgekonzeptes,

Kosten für die Realisierung und Aufrechterhaltung der den Betrieb begleitenden Notfallvorsorgemaßnahmen,  
Kosten für Notfallübungen und  
Kosten für die Wiederherstellung der Betriebsfähigkeit.

Der Aufwand zur Erstellung eines Notfallhandbuchs einschließlich der notwendigen begleitenden Maßnahmen ist beträchtlich.

---

Seite 21

Rheinlandtreffen 12.11.2008

---

Erstellung Notfallplan

---

Notfallplan

Das Notfallhandbuch muss im Notfall schnell erreichbar und transportabel sein.

Bei ausschließlich elektronischer Speicherung des Dokumentes oder wenn es in einer werkzeuggestützten Form vorliegt, ist die Bereitstellung eines oder mehrerer Notfall-Notebooks erforderlich.

---

Seite 22

Rheinlandtreffen 12.11.2008

---

Erstellung Notfallplan

---

Bei der Analyse, welche Bedrohung und Gefährdung für die IT existieren, stellt man schnell fest, dass z.B. die Gefährdung der IT durch ein Brand nicht nur die IT bedroht, sondern auch Mitarbeiter, kostbare Einrichtungen, gelagerte Produkte ...  
d.h. personelle Sicherheit ist bedroht.

Im Ernstfall müssen die entsprechenden Sicherheitsverantwortlichen für die Bereiche

Arbeitsschutz

Strahlenschutz

Umweltschutz

IT-Schutz

Geheimschutz

Objektschutz

reagieren

---

Seite 23

Rheinlandtreffen 12.11.2008

---

Erstellung Notfallplan

---

Incident-Management

Für welche Gefahren sollen Notfallpläne existieren ?

Medizinischer Notfall

Austritt von Gefahrstoffen

Feuer

Polizeilage

Sonstige Ereignisse

1. Stromausfall
2. Wasserausfall
3. Überschwemmung
4. Erdbeben
5. Flugzeugabsturz

....

---

Seite 24

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

Wachanweisungen

Seite 25

---

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---

Wachanweisungen

WER muß WANN informiert werden ?

WER ist weisungsbefugt ?

WER hat WANN WO Zutritt ?

Seite 26

---

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---


Wachanweisungen

- Medizinischer Notfall
  - Person leicht verletzt
  - Person lebensbedrohlich verletzt
- Austritt von Gefahrstoffen
  - Gasaustrittsmeldung
  - Gasaustritt
  - Austritt radioaktiver Stoffe
  - Austritt anderer Gefahrstoffe
- Feuer
  - Brandmeldung durch Brandmeldeanlage
  - Feuer im Gebäude
  - Feuer im Experimentalbereich
  - Feuer in Rechenzentrum
  - Feuer auf dem Parkplatz

---

Seite 27

Rheinlandtreffen 12.11.2008



**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---


Wachanweisungen

- Polizeilage
  - Bombendrohung
  - Einbruch (auch Hackerangriff)
  - Randalierer
  - Geiselnahme
  - Schutzperson/VIP
  - Verdächtiger Gegenstand
- Sonstige Ereignisse
  - Stromausfall
  - Ausfall Klimaanlage
  - Ausfall USVs
  - Wasserausfall
  - Überschwemmung
  - Sturmwarnung
  - Sturm
  - Schnee/Eis
  - Erdbeben
  - Flugzeugabsturz

---

Seite 28

Rheinlandtreffen 12.11.2008



**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---

Wachanweisungen

Notfall in der Dienstzeit

- wer ist im Haus ?
- bei Räumung des Hauses
  - wer ist noch im Gebäude ?
  - wer schaut nach ?


Notfall außerhalb der Dienstzeit

- Bereitschaftsdienst
- wer kommt ohne Bereitschaftsdienst ?

---

Seite 29

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---

„Kochrezept“ des BSI für ein Notfallhandbuch für den IT-Bereich

---

Seite 30

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

## Erstellung Notfallplan

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen](#)
- [M 6.2 Notfall-Definition, Notfall-Verantwortlicher](#)
- [M 6.3 Erstellung eines Notfall-Handbuchs](#)
- [M 6.4 Dokumentation der Kapazitätsanforderungen der IT-Anwendungen](#)
- [M 6.5 Definition des eingeschränkten IT-Betriebs](#)
- [M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten](#)
- [M 6.7 Regelung der Verantwortung im Notfall](#)
- [M 6.8 Alarmierungsplan](#)
- [M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse](#)
- [M 6.10 Notfall-Plan für DFÜ-Ausfall](#)
- [M 6.11 Erstellung eines Wiederanlaufplans](#)
- [M 6.12 Durchführung von Notfallübungen](#)
- [M 6.13 Erstellung eines Datensicherungsplans](#)
- [M 6.14 Ersatzbeschaffungsplan](#)
- [M 6.15 Lieferantenvereinbarungen](#)
- [M 6.16 Abschließen von Versicherungen](#)
- [M 6.17 Alarmierungsplan und Brandschutzübungen](#)
- [M 6.18 Redundante Leitungsführung](#)
- [M 6.19 Datensicherung am PC](#)
- [M 6.20 Geeignete Aufbewahrung der Backup-Datenträger](#)
- [M 6.21 Sicherungskopie der eingesetzten Software](#)
- [M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen](#)

Seite 31

Rheinlandtreffen 12.11.2008

## Erstellung Notfallplan

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.23 Verhaltensregeln bei Auftreten eines Computer-Virus](#)
- [M 6.24 Erstellen eines Notfall-Bootmediums](#)
- [M 6.25 Regelmäßige Datensicherung der Server-Festplatte](#)
- [M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten](#)
- [M 6.27 Sicheres Update des BIOS](#)
- [M 6.28 Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen](#)
- [M 6.29 TK-Basisanschluss für Notrufe](#)
- [M 6.30 Katastrophenschaltung](#)
- [M 6.31 Verhaltensregeln nach Verlust der Systemintegrität](#)
- [M 6.32 Regelmäßige Datensicherung](#)
- [M 6.33 Entwicklung eines Datensicherungskonzepts](#)
- [M 6.34 Erhebung der Einflussfaktoren der Datensicherung](#)
- [M 6.35 Festlegung der Verfahrensweise für die Datensicherung](#)
- [M 6.36 Festlegung des Minimaldatensicherungskonzeptes](#)
- [M 6.37 Dokumentation der Datensicherung](#)

Seite 32

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.38 Sicherungskopie der übermittelten Daten](#)
- [M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung](#)
- [M 6.40 Regelmäßige Batterieprüfung/-wechsel](#)
- [M 6.41 Übungen zur Datenrekonstruktion](#)
- [M 6.42 Erstellung von Rettungsdisketten für Windows NT](#)
- [M 6.43 Einsatz redundanter Windows NT/2000 Server](#)
- [M 6.44 Datensicherung unter Windows NT](#)
- [M 6.45 Datensicherung unter Windows 95](#)
- [M 6.46 Erstellung von Rettungsdisketten für Windows 95](#)
- [M 6.47 Aufbewahrung der Backup-Datenträger für Telearbeit](#)
- [M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität](#)
- [M 6.49 Datensicherung einer Datenbank](#)
- [M 6.50 Archivierung von Datenbeständen](#)
- [M 6.51 Wiederherstellung einer Datenbank](#)

---

Seite 33

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

Erstellung Notfallplan

---


**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.38 Sicherungskopie der übermittelten Daten](#)
- [M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung](#)
- [M 6.40 Regelmäßige Batterieprüfung/-wechsel](#)
- [M 6.41 Übungen zur Datenrekonstruktion](#)
- [M 6.42 Erstellung von Rettungsdisketten für Windows NT](#)
- [M 6.43 Einsatz redundanter Windows NT/2000 Server](#)
- [M 6.44 Datensicherung unter Windows NT](#)
- [M 6.45 Datensicherung unter Windows 95](#)
- [M 6.46 Erstellung von Rettungsdisketten für Windows 95](#)
- [M 6.47 Aufbewahrung der Backup-Datenträger für Telearbeit](#)
- [M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität](#)
- [M 6.49 Datensicherung einer Datenbank](#)
- [M 6.50 Archivierung von Datenbeständen](#)
- [M 6.51 Wiederherstellung einer Datenbank](#)
- [M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten](#)
- [M 6.53 Redundante Auslegung der Netzkomponenten](#)
- [M 6.54 Verhaltensregeln nach Verlust der Netzintegrität](#)

---

Seite 34

Rheinlandtreffen 12.11.2008

  
**Fraunhofer** Institut  
Naturwissenschaftlich-  
Technische Trendanalysen

## Erstellung Notfallplan

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.55 Reduzierung der Wiederanlaufzeit für Novell Netware Server](#)
- [M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren](#)
- [M 6.57 Erstellen eines Notfallplans für den Ausfall des Managementsystems](#)
- [M 6.58 Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen](#)
- [M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen](#)
- [M 6.60 Verhaltensregeln und Meldewege bei Sicherheitsvorfällen](#)
- [M 6.61 Eskalationsstrategie für Sicherheitsvorfälle](#)
- [M 6.62 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen](#)
- [M 6.63 Untersuchung und Bewertung eines Sicherheitsvorfalls](#)
- [M 6.64 Behebung von Sicherheitsvorfällen](#)
- [M 6.65 Benachrichtigung betroffener Stellen](#)
- [M 6.66 Nachbereitung von Sicherheitsvorfällen](#)
- [M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle](#)
- [M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen](#)
- [M 6.69 Notfallvorsorge und Ausfallsicherheit bei Faxservern](#)
- [M 6.70 Erstellen eines Notfallplans für den Ausfall des RAS-Systems](#)
- [M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems](#)

Seite 35

Rheinlandtreffen 12.11.2008

## Erstellung Notfallplan

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.72 Ausfallvorsorge bei Mobiltelefonen](#)
- [M 6.73 Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems](#)
- [M 6.74 Notfallarchiv](#)
- [M 6.75 Redundante Kommunikationsverbindungen](#)
- [M 6.76 Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes](#)
- [M 6.77 Erstellung von Rettungsdisketten für Windows 2000](#)
- [M 6.78 Datensicherung unter Windows 2000/XP](#)
- [M 6.79 Datensicherung beim Einsatz von Internet-PCs](#)
- [M 6.80 Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes](#)
- [M 6.81 Erstellen von Datensicherungen für Novell eDirectory](#)
- [M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen](#)
- [M 6.83 Notfallvorsorge beim Outsourcing](#)
- [M 6.84 Regelmäßige Datensicherung der System- und Archivdaten](#)
- [M 6.85 Erstellung eines Notfallplans für den Ausfall des IIS](#)
- [M 6.86 Schutz vor schädlichem Code auf dem IIS](#)
- [M 6.87 Datensicherung auf dem IIS](#)
- [M 6.88 Erstellen eines Notfallplans für den Webserver](#)
- [M 6.89 Notfallvorsorge für einen Apache-Webserver](#)
- [M 6.90 Datensicherung und Archivierung von E-Mails](#)

Seite 36

Rheinlandtreffen 12.11.2008

Erstellung Notfallplan

---

**M 6 Maßnahmenkatalog Notfallvorsorge nach BSI**

- [M 6.91 Datensicherung und Recovery bei Routern und Switches](#)
- [M 6.92 Notfallvorsorge bei Routern und Switches](#)
- [M 6.93 Notfallvorsorge für z/OS-Systeme](#)
- [M 6.94 Notfallvorsorge bei Sicherheitsgateways](#)
- [M 6.95 Ausfallvorsorge und Datensicherung bei PDAs](#)
- [M 6.96 Notfallvorsorge für einen Server](#)
- [M 6.97 Notfallvorsorge für SAP Systeme](#)
- [M 6.98 Notfallvorsorge für Speichersysteme](#)
- [M 6.99 Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003](#)
- [M 6.100 Erstellung eines Notfallplans für den Ausfall von VoIP](#)
- [M 6.101 Datensicherung bei VoIP](#)
- [M 6.102 Verhaltensregeln bei WLAN-Sicherheitsvorfällen](#)
- [M 6.103 Redundanzen für die Primärverkabelung](#)
- [M 6.104 Redundanzen für die Gebäudeverkabelung](#)
- [M 6.105 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten](#)

---

Seite 37

Rheinlandtreffen 12.11.2008



Erstellung Notfallplan

---

**Fragen ?**

---

Seite 38

Rheinlandtreffen 12.11.2008

