<Kundenname>

IT-Disaster-Recovery-Plan

Vorlage

# *Von Paul Kirvan, CISA, CISSP, FBCI, CBCP*

**Geschichte der Revision**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Datum | Name | Beschreibung |
| Original 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsübersicht**

[Absichtserklärung zur Informationstechnologie 5](#_Toc241554706)

[Grundsatzerklärung 5](#_Toc241554707)

[Zielsetzungen 5](#_Toc241554708)

[Kontaktinformationen für wichtige Mitarbeiter 6](#_Toc241554709)

[Benachrichtigung Rufbaum 7](#_Toc241554710)

[Externe Kontakte 8](#_Toc241554711)

[Externe Kontakte Anruferliste 10](#_Toc241554712)

[1 Plan Übersicht 11](#_Toc241554713)

[1.1 Planaktualisierung 11](#_Toc241554714)

[1.2 Speicherung der Plandokumentation 11](#_Toc241554715)

[1.3 Backup-Strategie 11](#_Toc241554716)

[1.4 Risikomanagement 11](#_Toc241554717)

[2 Notfallmaßnahmen 12](#_Toc241554718)

[2.1 Alarmierung, Eskalation und Planaufruf 12](#_Toc241554719)

[2.1.1 Auslösende Ereignisse planen 12](#_Toc241554720)

[2.1.2 Versammlungspunkte 12](#_Toc241554721)

[2.1.3 Aktivierung des Notfallteams 12](#_Toc241554722)

[2.2 Disaster Recovery Team 13](#_Toc241554723)

[2.3 Notfallalarm, Eskalation und DRP-Aktivierung 13](#_Toc241554724)

[2.3.1 Notfallalarm 13](#_Toc241554725)

[2.3.2 DR-Verfahren für das Management 14](#_Toc241554726)

[2.3.3 Kontakt mit Mitarbeitern 14](#_Toc241554727)

[2.3.4 Backup-Personal 14](#_Toc241554728)

[2.3.5 Aufgezeichnete Nachrichten / Updates 14](#_Toc241554729)

[2.3.7 Alternative Wiederherstellungseinrichtungen / Hot Site 14](#_Toc241554730)

[2.3.8 Personal und Familie Benachrichtigung 14](#_Toc241554731)

[3 Medien 15](#_Toc241554732)

[3.1 Medienkontakt 15](#_Toc241554733)

[3.2 Medien-Strategien 15](#_Toc241554734)

[3.3 Medien-Team 15](#_Toc241554735)

[3.4 Regeln für den Umgang mit den Medien 15](#_Toc241554736)

[4 Versicherung 15](#_Toc241554737)

[5 Finanzielle und rechtliche Fragen 16](#_Toc241554738)

[5.1 Finanzielle Bewertung 16](#_Toc241554739)

[5.2 Finanzielle Anforderungen 16](#_Toc241554740)

[5.3 Rechtliche Schritte 16](#_Toc241554741)

[6 DRP-Übung 16](#_Toc241554742)

[Anhang A - Vorlagen für einen Disaster-Recovery-Plan für Technologie 17](#_Toc241554743)

[Disaster Recovery Plan für <System Eins> 17](#_Toc241554744)

[Notfallwiederherstellungsplan für <System Zwei> 19](#_Toc241554745)

[Notfallwiederherstellungsplan für ein lokales Netzwerk (LAN) 21](#_Toc241554746)

[Notfallwiederherstellungsplan für Wide Area Network (WAN) 23](#_Toc241554747)

[Disaster-Recovery-Plan für Remote-Konnektivität 25](#_Toc241554748)

[Disaster Recovery Plan für Sprachkommunikation 27](#_Toc241554749)

[Anhang B - Vorgeschlagene Formulare 29](#_Toc241554750)

[Formular zur Schadensbewertung 29](#_Toc241554751)

[Formular Management von DR-Aktivitäten 29](#_Toc241554752)

[Formular zur Aufzeichnung von Disaster-Recovery-Ereignissen 29](#_Toc241554753)

[Formular für den Bericht über die DR-Aktivitäten 30](#_Toc241554754)

[Formular zur Mobilisierung des Disaster Recovery Teams 31](#_Toc241554755)

[Mobilisierung des Business Recovery Team Formular 31](#_Toc241554756)

[Formular zur Überwachung des Fortschritts von Wiederherstellungsaufgaben 32](#_Toc241554757)

[Vorbereitung des Formulars für den Bericht über die Sanierung von Unternehmen 32](#_Toc241554758)

[Formular Kommunikation 33](#_Toc241554759)

[Rückführung wiederhergestellter Geschäftsabläufe in die Führung der Geschäftseinheit 33](#_Toc241554760)

[Formular zur Wiederherstellung von Geschäftsprozessen/Funktionen 33](#_Toc241554761)

# **Absichtserklärung zur Informationstechnologie**

In diesem Dokument werden unsere Richtlinien und Verfahren für das Disaster Recovery sowie unsere Pläne auf Prozessebene für die Wiederherstellung kritischer Technologieplattformen und der Telekommunikationsinfrastruktur dargelegt. Dieses Dokument fasst die von uns empfohlenen Verfahren zusammen. Im Falle einer tatsächlichen Notfallsituation können Änderungen an diesem Dokument vorgenommen werden, um die physische Sicherheit unserer Mitarbeiter, unserer Systeme und unserer Daten zu gewährleisten.

Unsere Aufgabe ist es, die Betriebszeit von Informationssystemen, die Datenintegrität und -verfügbarkeit sowie die Geschäftskontinuität sicherzustellen.

# **Grundsatzerklärung**

Die Unternehmensleitung hat die folgende Grundsatzerklärung genehmigt:

* Das Unternehmen entwickelt einen umfassenden IT-Disaster-Recovery-Plan.
* Es wird eine formelle Risikobewertung durchgeführt, um die Anforderungen an den DR-Plan zu bestimmen.
* Der Disaster-Recovery-Plan sollte alle wesentlichen und kritischen Infrastrukturelemente, Systeme und Netze in Übereinstimmung mit den Hauptgeschäftsaktivitäten abdecken.
* Der DR-Plan sollte regelmäßig in einer simulierten Umgebung getestet werden, um sicherzustellen, dass er in Notfallsituationen umgesetzt werden kann und dass das Management und die Mitarbeiter verstehen, wie er ausgeführt werden soll.
* Alle Mitarbeiter müssen mit dem DR-Plan und ihren jeweiligen Aufgaben vertraut gemacht werden.
* Der DR-Plan muss auf dem neuesten Stand gehalten werden, um veränderten Umständen Rechnung zu tragen.

# **Zielsetzungen**

Das Hauptziel des Disaster-Recovery-Programms besteht darin, einen gut strukturierten und leicht verständlichen Plan zu entwickeln, zu testen und zu dokumentieren, der dem Unternehmen hilft, sich so schnell und effektiv wie möglich von einer unvorhergesehenen Katastrophe oder einem Notfall zu erholen, der die Informationssysteme und den Geschäftsbetrieb unterbricht. Zu den weiteren Zielen gehören folgende:

* Die Notwendigkeit, sicherzustellen, dass alle Mitarbeiter ihre Pflichten bei der Umsetzung eines solchen Plans vollständig verstehen.
* Die Notwendigkeit, sicherzustellen, dass bei allen geplanten Aktivitäten die operativen Strategien eingehalten werden.
* Die Notwendigkeit, sicherzustellen, dass die vorgeschlagenen Notfallvorkehrungen kosteneffizient sind.
* Die Notwendigkeit, die Auswirkungen auf andere Unternehmensstandorte zu berücksichtigen.
* Disaster-Recovery-Funktionen für wichtige Kunden, Lieferanten und andere externe Kontakte zu entwickeln.

# **Kontaktinformationen für wichtige Mitarbeiter**

| **Name, Titel** | **Kontakt Option** | **Kontakt Nummer** |
| --- | --- | --- |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |
|  | Arbeit |  |
|  | Alternative |  |
|  | Mobil |  |
|  | Startseite |  |
|  | E-Mail Adresse |  |
|  | Alternative E-Mail |  |
|  |  |  |

## **Benachrichtigung Anrufbaum**

Person, die den Vorfall identifiziert

# **Externe Kontakte**

| **Name, Titel** | | **Kontakt Option** | | **Kontakt Nummer** |
| --- | --- | --- | --- | --- |
| **Vermieter / Hausverwalter** | |  | |  |
| Kontonummer Keine | |  | |  |
|  | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Startseite | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Energieversorgungsunternehmen** | |  | |  |
| Kontonummer | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Startseite | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Telekom-Betreiber 1** | |  | |  |
| Kontonummer | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Fax | |  |
|  | | Startseite | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Telekom-Betreiber 2** | |  | |  |
| Kontonummer | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Startseite | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Hardware-Lieferant 1** | |  | |  |
| Kontonummer | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Meldung von Notfällen | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Server-Lieferant 1** | |  | |  |
| Kontonummer. | | Arbeit | |  |
|  | | Mobil | |  |
|  | | Fax | |  |
|  | | E-Mail Adresse | |  |
|  | |  | |  |
| **Arbeitsplatz Lieferant 1** | |  |  | |
| Kontonummer | | Arbeit |  | |
|  | | Mobil |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
|  | |  |  | |
| **Büromaterial 1** | |  |  | |
| Kontonummer C3095783 | | Arbeit |  | |
|  | | Mobil |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
| **Versicherung - Name** | |  |  | |
| Kontonummer | | Arbeit |  | |
|  | | Mobil |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
|  | |  |  | |
| **Sicherheit vor Ort -** | |  |  | |
| Kontonummer | | Arbeit |  | |
|  | | Mobil |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
|  | |  |  | |
| **Off-Site-Lagerung 1** | |  |  | |
| Kontonummer | | Arbeit |  | |
|  | | Mobil |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
|  | |  |  | |
| **Off-Site-Lagerung 2** | |  |  | |
| Kontonummer | | Benutzer-ID |  | |
|  | | Passwort |  | |
|  | | Startseite |  | |
|  | | E-Mail Adresse |  | |
|  | |  |  | |
| **HLK (HVAC)** |  | |  | |
| Kontonummer | Arbeit | |  | |
|  | Mobil | |  | |
|  | Startseite | |  | |
|  | E-Mail Adresse | |  | |
|  |  | |  | |
| **Stromerzeuger** |  | |  | |
| Kontonummer | Arbeit | |  | |
|  | Mobil | |  | |
|  | Startseite | |  | |
|  | E-Mail Adresse | |  | |
|  |  | |  | |
| **Sonstiges** |  | |  | |
| Kontonummer | Arbeit | |  | |
|  | Mobil | |  | |
|  | Startseite | |  | |
|  | E-Mail Adresse | |  | |
|  |  | |  | |

## **Externe Kontakte Anruferliste**

# **1 Plan Übersicht**

## **1.1 Planaktualisierung**

Es ist notwendig, dass der Prozess der DRP-Aktualisierung angemessen strukturiert und kontrolliert wird. Wann immer Änderungen am Plan vorgenommen werden, müssen sie vollständig getestet werden, und es sollten entsprechende Änderungen an den Schulungsmaterialien vorgenommen werden. Dies umfasst die Anwendung formalisierter Änderungskontrollverfahren unter der Kontrolle des IT-Direktors

## **1.2 Speicherung der Plandokumentation**

Kopien dieses Plans, CD und Ausdrucke werden an sicheren, vom Unternehmen festzulegenden Orten aufbewahrt. Jedes Mitglied der Geschäftsleitung erhält eine CD und einen Ausdruck dieses Plans, die zu Hause aufbewahrt werden. Jedes Mitglied des Disaster Recovery Teams und des Business Recovery Teams erhält eine CD und einen Ausdruck dieses Plans. Eine geschützte Masterkopie wird auf speziellen, zu diesem Zweck eingerichteten Ressourcen gespeichert.

## **1.3 Backup-Strategie**

Die wichtigsten Geschäftsprozesse und die jeweils vereinbarte Backup-Strategie sind nachstehend aufgeführt. Die gewählte Strategie sieht einen vollständig gespiegelten Wiederherstellungsstandort in den Geschäftsräumen des Unternehmens in \_\_\_\_\_ vor. Diese Strategie enthält die Unterhaltung eines vollständig gespiegelten Duplikats des Standorts, das einen sofortigen Wechsel zwischen dem Live-Standort (Hauptsitz) und dem Backup-Standort ermöglicht (Failover).

|  |  |
| --- | --- |
| **ZENTRALER GESCHÄFTSPROZESS** | **BACKUP-STRATEGIE** |
| IT-Betrieb | Vollständig gespiegelter Wiederherstellungsstandort |
| Technische Unterstützung - Hardware | Vollständig gespiegelter Wiederherstellungsstandort |
| Technische Unterstützung - Software | Vollständig gespiegelter Wiederherstellungsstandort |
| Gebäudemanagement | Vollständig gespiegelter Wiederherstellungsstandort |
| E-Mail | Vollständig gespiegelter Wiederherstellungsstandort |
| Einkaufen | Vollständig gespiegelter Wiederherstellungsstandort |
| Wiederherstellung im Katastrophenfall | Vollständig gespiegelter Wiederherstellungsstandort |
| Finanzen | Vollständig gespiegelter Wiederherstellungsstandort |
| Verwaltung von Verträgen | Vollständig gespiegelter Wiederherstellungsstandort |
| Lager & Inventar | Vollständig gespiegelter Wiederherstellungsstandort |
| Produktverkäufe | Vollständig gespiegelter Wiederherstellungsstandort |
| Wartung Verkauf | Vollständig gespiegelter Wiederherstellungsstandort |
| Personalwesen | Datenspeicher außerhalb des Standorts |
| Testen einer vollständig gespiegelten Wiederherstellungsseite - | Vollständig gespiegelter Wiederherstellungsstandort |
| Workshop Vollständig gespiegelter Wiederherstellungsstandort - | Vollständig gespiegelter Wiederherstellungsstandort |
| Call Center | Vollständig gespiegelter Wiederherstellungsstandort |
|  | Vollständig gespiegelter Wiederherstellungsstandort |

## **1.4 Risikomanagement**

Es gibt viele potenzielle Bedrohungen, die jederzeit auftreten und den normalen Geschäftsablauf beeinträchtigen können. Wir haben ein breites Spektrum potenzieller Bedrohungen in Betracht gezogen, und die Ergebnisse unserer Überlegungen sind in diesem Abschnitt enthalten. Jede potenzielle Umweltkatastrophe oder Notfallsituation wurde untersucht. Der Schwerpunkt liegt dabei auf dem Ausmaß der Betriebsunterbrechung, die sich aus jeder Art von Katastrophe ergeben könnte

Die potenziellen Katastrophen wurden wie folgt bewertet:

|  |  |  |  |
| --- | --- | --- | --- |
| **Potenzielle Katastrophe** | **Bewertung der Wahrscheinlichkeit** | **Bewertung der Auswirkungen** | **Kurze Beschreibung der möglichen Folgen und Abhilfemaßnahmen** |
| Hochwasser | 3 | 4 | Alle wichtigen Geräte befinden sich im 1. Stock |
| Feuer | 3 | 4 | FM200-Unterdrückungssystem in den Hauptrechenzentren installiert. Brand- und Rauchmelder auf allen Etagen. |
| Tornado | 5 |  |  |
| Elektrische Stürme | 5 |  |  |
| Terroristischer Akt | 5 |  |  |
| Akt der Sabotage | 5 |  |  |
| Elektrische Leistung  Ausfall | 3 | 4 | Redundante USV-Anlage zusammen mit automatischem Notstromgenerator, der wöchentlich getestet und rund um die Uhr fernüberwacht wird. USVs auch aus der Ferne überwacht. |
| Ausfall von Kommunikationsnetzdiensten | 4 | 4 | Zwei vielfältig geroutete T1-Leitungen ins Gebäude. WAN-Redundanz, Ausfallsicherheit des Sprachnetzes |

Wahrscheinlichkeit: 1=Sehr hoch, 5=Sehr niedrig Auswirkung: 1=Totale Zerstörung, 5=Minimale Störung

# **2 Notfallmaßnahmen**

## **2.1 Alarmierung, Eskalation und Planaufruf**

### 2.1.1 Auslösende Ereignisse planen

Die wichtigsten Auslöser im Hauptstandort, die zur Aktivierung des DRP führen würden, sind

* Totalausfall der Kommunikation
* Totalausfall der Stromversorgung
* Überflutung der Räumlichkeiten
* Verlust des Gebäudes

### 2.1.2 Versammlungspunkte

Für den Fall, dass die Räumlichkeiten evakuiert werden müssen, sieht der DRP-Aufrufplan zwei Evakuierungssammelstellen vor:

* Primär - Ganz am Ende des Hauptparkplatzes;
* Alternative - Parkplatz des Unternehmens auf der anderen Straßenseite

### 2.1.3 Aktivierung des Notfallteams (Emergency Response Team)

Wenn ein Zwischenfall eintritt, muss das Emergency Response Team (ERT) aktiviert werden. Das ERT entscheidet dann, inwieweit der DR-Plan in Anspruch genommen werden muss. Alle Mitarbeiter müssen eine Schnellreferenzkarte mit den Kontaktdaten des ERT erhalten, die im Katastrophenfall zu verwenden ist. Die Aufgaben des ERT sind:

* sofort auf eine mögliche Katastrophe zu reagieren und den Notdienst zu rufen.
* das Ausmaß der Katastrophe zu beurteilen und ihre Auswirkungen auf das Unternehmen, das Rechenzentrum zu bewerten.
* zu entscheiden, welche Elemente des DR-Plans aktiviert werden sollen.
* ein Disaster-Recovery-Teams zur Aufrechterhaltung lebenswichtiger Dienste und zur Wiederherstellung des Normalbetriebs zusammenzusetzen und zu leiten.
* sicherzustellen, dass die Mitarbeiter informiert werden, und Zuständigkeiten und Tätigkeiten nach Bedarf zuzuweisen.

## **2.2 Disaster Recovery Team**

Das Team wird vom ERT kontaktiert und zusammengestellt. Zu den Aufgaben des Teams gehören:

* Schaffung von Einrichtungen für einen Notdienst innerhalb von 2,0 Geschäftsstunden.
* Wiederherstellung der wichtigsten Dienste innerhalb von 4,0 Geschäftsstunden nach dem Vorfall.
* Wiederherstellung des normalen Betriebs innerhalb von 8,0 bis 24,0 Stunden nach dem Vorfall.
* Koordinierung der Aktivitäten mit dem Katastrophenschutzteam, den Ersthelfern und anderen Ressourcen.
* Reports an das Notfallteam (ERT) weitergeben.

## **2.3 Notfallalarm, Eskalation und DRP-Aktivierung**

Diese Richtlinien und Verfahren wurden eingeführt, um sicherzustellen, dass das Personal im Falle einer Katastrophe oder Krise genau weiß, wer zu kontaktieren ist. Verfahren wurden eingeführt, um sicherzustellen, dass die Kommunikation während der Aktivierung des Disaster Recoverys schnell hergestellt werden kann.

Der DR-Plan stützt sich in erster Linie auf Mitglieder der Geschäftsleitung und Mitarbeiter in Schlüsselpositionen, die die für eine reibungslose Wiederherstellung der Technologie und des Geschäftsbetriebs erforderlichen technischen und verwaltungstechnischen Fähigkeiten mitbringen. Die Lieferanten kritischer Güter und Dienstleistungen werden die Wiederherstellung des Geschäftsbetriebs weiterhin unterstützen, wenn das Unternehmen zum normalen Betriebsmodus zurückkehrt.

### 2.3.1 Notfallalarm

Die Person, die den Vorfall entdeckt, ruft ein Mitglied des Notfallteams (ERT) in der angegebenen Reihenfolge an:

Emergency Response Team

- \_\_\_\_\_\_\_\_\_

- \_\_\_\_\_\_\_\_\_

- \_\_\_\_\_\_\_\_\_

Falls nicht verfügbar, versuchen Sie es:

- \_\_\_\_\_\_\_\_\_

- \_\_\_\_\_\_\_\_\_

Das Emergency Response Team (ERT) ist verantwortlich für die Aktivierung des DRP bei den durch diesem Plan identifizierten Katastrophen sowie bei allen anderen Ereignissen, die den normalen Geschäftsbetrieb des Unternehmens, beeinträchtigen.

Eine der Aufgaben in der Anfangsphase des Notfalls ist die Benachrichtigung des Disaster Recovery Teams (DRT), dass ein Notfall eingetreten ist. In der Benachrichtigung werden die Mitglieder des DRT aufgefordert, sich am Ort des Problems zu versammeln, und es werden ausreichende Informationen übermittelt, um diese Aufforderung wirksam zu übermitteln. Das Business Recovery Team (BRT) besteht aus leitenden Vertretern der wichtigsten Unternehmensabteilungen. Der Leiter des BRT ist ein hochrangiges Mitglied des Managementteams des Unternehmens und hat die Aufgabe, die Gesamtleitung des Prozesses zu übernehmen und sicherzustellen, dass das Unternehmen so schnell wie möglich zum normalen Arbeitsbetrieb zurückkehrt

### 2.3.2 DR-Verfahren für das Management

Die Mitglieder des Managementteams bewahren die Namen und Kontaktnummern aller Mitarbeiter ihrer Abteilungen in Papierform auf. Darüber hinaus haben die Mitglieder des Managementteams einen Ausdruck der DR- und Geschäftskontinuitätspläne des Unternehmens bei sich zu Hause aufbewahrt, für den Fall, dass das Gebäude des Hauptsitzes unzugänglich, unbrauchbar oder zerstört ist

### 2.3.3 Kontakt mit Mitarbeitern

Die Führungskräfte fungieren als Ansprechpartner für ihre Abteilungen, während bestimmte Mitarbeiter andere Mitarbeiter anrufen, um die Krise/Katastrophe und die unmittelbaren Pläne des Unternehmens zu besprechen. Mitarbeiter, die die Mitarbeiter auf ihrer Anrufliste nicht erreichen können, sollten den Notfallkontakt des Mitarbeiters anrufen, um Informationen über die Katastrophe weiterzugeben.

### 2.3.4 Backup-Personal

Wenn ein Vorgesetzter oder ein Mitarbeiter, der für die Kontaktaufnahme mit anderen Mitarbeitern zuständig ist, nicht verfügbar oder verhindert ist, übernimmt der benannte Ersatzmitarbeiter die Benachrichtigungsaufgaben

### 2.3.5 Aufgezeichnete Nachrichten / Updates

Für die neuesten Informationen über die Katastrophe und die Reaktion der Organisation können die Mitarbeiter eine gebührenfreie Hotline anrufen, die im DRP aufgeführt ist. Die Nachrichten enthalten Angaben über die Art der Katastrophe, die Sammelstellen und aktuelle Informationen über die Wiederaufnahme der Arbeit.

### 2.3.7 Alternative Recovery-Standorte / Hot Site

Falls erforderlich, wird der Hot Site bei SunGard aktiviert und die Benachrichtigung erfolgt über aufgezeichnete Nachrichten oder durch Kommunikation mit den Managern. In den ersten 24 Stunden werden nur Mitglieder des DR-Teams am Notfallort tätig , danach werden bei Bedarf weitere zum Notfallort kommen.

### 2.3.8 Benachrichtigung von Personal und Familie

Wenn der Vorfall zu einer Situation geführt hat, die für die unmittelbaren Angehörigen eines Mitarbeiters besorgniserregend ist, wie zum Beispiel die Einlieferung von Verletzten in ein Krankenhaus, müssen die unmittelbaren Familienangehörigen schnell benachrichtigt werden

# **3 Medien**

## **3.1 Medienkontakt**

Das zugewiesene Personal wird sich mit den Medien abstimmen und dabei nach den zuvor genehmigten und herausgegebenen Richtlinien für die Kommunikation nach Katastrophen arbeiten.

## **3.2 Medien-Strategien**

1. Vermeidung von negativer Publicity
2. Nutzen Sie die Gelegenheiten für nützliche Werbung
3. Antworten auf die folgenden grundlegenden Fragen haben:
   * Was ist passiert?
   * Wie ist es dazu gekommen?
   * Was werden Sie dagegen tun?

## **3.3 Medien-Team**

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **3.4 Regeln für den Umgang mit den Medien**

**Nur** dem Medienteam ist der direkte Kontakt mit den Medien gestattet; alle anderen Kontaktpersonen sollten Anrufer oder persönliche Medienvertreter an das Medienteam verweisen.

# **4 Versicherung**

Im Rahmen Unternehmensstrategie für Disaster Recovery und Business Continuity wurde eine Reihe von Versicherungs- Policen abgeschlossen. Dazu gehören eine Versicherung für Fehler und Unterlassungen, eine Haftpflichtversicherung für Geschäftsführer und leitende Angestellte, eine allgemeine Haftpflichtversicherung und eine Betriebsunterbrechungsversicherung.

*Wenn Sie in einem Notfall außerhalb der normalen Geschäftszeiten versicherungsbezogene Hilfe benötigen, wenden Sie sich bitte an: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Policy-Name** | **Art der Deckung** | **Erfassungszeitraum** | **Höhe der Deckungssumme** | **Verantwortliche Person**  **Für Deckung** | **Nächste Erneuerung**  **Datum** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **5 Finanzielle und rechtliche Fragen**

## **5.1 Finanzielle Bewertung**

Das Notfallteam (ERT) erstellt eine erste Bewertung der Auswirkungen des Vorfalls auf die finanziellen Angelegenheiten des Unternehmens. Die Bewertung sollte Folgendes umfassen:

* Verlust von Finanzdokumenten
* Einnahmeverluste
* Diebstahl von Scheckbüchern, Kreditkarten und ähnlichen Wertgegenständen
* Verlust von Bargeld

## **5.2 Finanzielle Anforderungen**

Der unmittelbare Finanzbedarf des Unternehmens muss gedeckt werden. Dazu können gehören:

* Cashflow-Position
* Befristete Kreditaufnahmefähigkeit
* Anstehende Zahlungen für Steuern, Lohnsteuer, Sozialversicherung und andere Verpflichtungen
* Verfügbarkeit von Firmenkreditkarten zur Bezahlung der nach der Katastrophe benötigten Lieferungen und Dienstleistungen

## **5.3 Rechtliche Schritte**

Die Rechtsabteilung des Unternehmens und das ERT prüfen gemeinsam die Folgen des Vorfalls und entscheiden, ob sich aus dem Ereignis rechtliche Schritte ergeben können, insbesondere die Möglichkeit von Ansprüchen durch oder gegen das Unternehmen wegen Verstößen gegen Rechtsvorschriften oder andere Rechtsansprüche.

# **6 DRP-Übung**

Übungen des DR-Plans sind ein wesentlicher Bestandteil der Planentwicklung. Bei einer DRP-Übung gibt es kein Bestehen oder Durchfallen; jeder, der daran teilnimmt, lernt aus den Übungen: was verbessert werden muss und wie die Verbesserungen umgesetzt werden können. Planübungen stellen sicher, dass die Notfallteams mit ihren Aufgaben vertraut sind und, was noch wichtiger ist, dass sie Vertrauen in ihre Fähigkeiten haben.

Erfolgreiche DR-Pläne treten reibungslos und effektiv in Aktion, wenn sie benötigt werden. Dies ist nur möglich, wenn jeder, der in dem Plan eine Rolle zu spielen hat, diese Rolle ein oder mehrere Male geprobt hat. Der Plan sollte auch validiert werden, indem die Umstände, unter denen er funktionieren muss, simuliert werden, um zu sehen, was passiert

# **Anhang A - Vorlagen für technologische Notfallpläne**

## **Disaster Recovery Plan für <System One>**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| PRODUKTIONSSERVER | Standort:  Server-Modell:  Betriebssystem:  CPUs:  Gedächtnis:  Total Disk:  System-Handle:  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| HOT-SITE-SERVER | Details bereitstellen |
| ANWENDUNGEN  (Fettdruck für Hot Site) |  |
| ZUGEHÖRIGE SERVER |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |

|  |  |
| --- | --- |
| SICHERUNGSSTRATEGIE FÜR SYSTEM EINS |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM EINS** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust von Daten | Details bereitstellen |
| Szenario 2  Totalverlust von HW | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Dateisysteme <Datum>**

|  |  |
| --- | --- |
| **Dateisystem ab <Datum>**  Minimale Dateisysteme, die aus der Sicherung erstellt und wiederhergestellt werden müssen: | **Dateisystem kbytes Verwendet Verfügbar %verwendet Eingebunden in**  <Details bereitstellen> |
| Andere wichtige zu ändernde Dateien | <Details bereitstellen> |
| Erforderliche Verzeichnisse zum Erstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherzustellende Sekundärdateien | <Details bereitstellen> |
| Andere Dateien zum Wiederherstellen | <Details bereitstellen> |

## **Notfallwiederherstellungsplan für <System Zwei>**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| PRODUKTIONSSERVER | Standort:  Server-Modell:  Betriebssystem:  CPUs:  Gedächtnis:  Total Disk:  System-Handle:  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| HOT-SITE-SERVER | Details bereitstellen |
| ANWENDUNGEN  (Fettdruck für Hot Site) |  |
| ZUGEHÖRIGE SERVER |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |

|  |  |
| --- | --- |
| BACKUP-STRATEGIE für SYSTEM ZWEI |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM ZWEI** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust von Daten | Details bereitstellen |
| Szenario 2  Totalverlust von HW | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Dateisysteme <Datum>**

|  |  |
| --- | --- |
| Dateisystem ab <Datum>  Minimale Dateisysteme, die aus der Sicherung erstellt und wiederhergestellt werden müssen: | **Dateisystem kbytes Verwendet Verfügbar %verwendet Eingebunden in**  bereitstellen> |
| Andere wichtige zu ändernde Dateien | <Details bereitstellen> |
| Erforderliche Verzeichnisse zum Erstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherzustellende Sekundärdateien | <Details bereitstellen> |
| Andere Dateien zum Wiederherstellen | <Details bereitstellen> |

## **Disaster-Recovery-Plan für ein lokales Netzwerk (LAN)**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| SERVER | Standort:  Server-Modell:  Betriebssystem:  CPUs:  Gedächtnis:  Total Disk:  System-Handle:  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| HOT-SITE-SERVER | Details bereitstellen |
| ANWENDUNGEN  (Fettdruck für Hot Site) |  |
| ZUGEHÖRIGE SERVER |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |

|  |  |
| --- | --- |
| BACKUP-STRATEGIE für SYSTEM ZWEI |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM ZWEI** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust von Daten | Details bereitstellen |
| Szenario 2  Totalverlust von HW | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Dateisysteme <Datum>**

|  |  |
| --- | --- |
| Dateisystem ab <Datum>  Minimale Dateisysteme, die aus der Sicherung erstellt und wiederhergestellt werden müssen: | **Dateisystem kbytes Verwendet Verfügbar %verwendet Eingebunden in**  bereitstellen> |
| Andere wichtige zu ändernde Dateien | <Details bereitstellen> |
| Erforderliche Verzeichnisse zum Erstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherzustellende Sekundärdateien | <Details bereitstellen> |
| Andere Dateien zum Wiederherstellen | <Details bereitstellen> |

## **Disaster-Recovery-Plan für ein Wide Area Network (WAN)**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| AUSRÜSTUNG | Standort:  Gerätetyp:  Modell Nr.:  Technische Daten:  Netzwerk-Schnittstellen:  Leistungsanforderungen;  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| AUSRÜSTUNG FÜR HOT SITES | Details bereitstellen |
| SPEZIELLE ANWENDUNGEN |  |
| ZUGEHÖRIGE GERÄTE |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |
| Netzdienste | Details bereitstellen |

|  |  |
| --- | --- |
| BACKUP-STRATEGIE für SYSTEM ZWEI |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM ZWEI** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust des Netzes | Details bereitstellen |
| Szenario 2  Totalverlust von HW | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Unterstützungssysteme <Datum>**

|  |  |
| --- | --- |
| Unterstützungssystem | <Details bereitstellen> |
| Kritische Netzwerte | <Details bereitstellen> |
| Kritische Schnittstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherstellung kritischer Netzwerkdienste | <Details bereitstellen> |
| Sonstige Dienstleistungen | <Details bereitstellen> |

## **Disaster-Recovery-Plan für Remote-Konnektivität**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| AUSRÜSTUNG | Standort:  Gerätetyp:  Modell Nr.:  Technische Daten:  Netzwerk-Schnittstellen:  Leistungsanforderungen;  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| AUSRÜSTUNG FÜR HOT SITES | Details bereitstellen |
| SPEZIELLE ANWENDUNGEN |  |
| ZUGEHÖRIGE GERÄTE |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |
| Netzdienste | Details bereitstellen |

|  |  |
| --- | --- |
| BACKUP-STRATEGIE für SYSTEM ZWEI |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM ZWEI** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust des Netzes | Details bereitstellen |
| Szenario 2  Totalverlust von HW | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Unterstützungssysteme <Datum>**

|  |  |
| --- | --- |
| Unterstützungssystem | <Details bereitstellen> |
| Kritische Netzwerte | <Details bereitstellen> |
| Kritische Schnittstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherstellung kritischer Netzwerkdienste | <Details bereitstellen> |
| Sonstige Dienstleistungen | <Details bereitstellen> |

## **Disaster-Recovery-Plan für Sprachkommunikation**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| ÜBERBLICK |  |
| AUSRÜSTUNG | Standort:  Gerätetyp:  Modell Nr.:  Technische Daten:  Netzwerk-Schnittstellen:  Leistungsanforderungen;  System-Seriennummer:  DNS-Eintrag:  IP-Adresse:  Sonstiges: |
| AUSRÜSTUNG FÜR HOT SITES | Details bereitstellen |
| SPEZIELLE ANWENDUNGEN |  |
| ZUGEHÖRIGE GERÄTE |  |

|  |  |
| --- | --- |
| SCHLÜSSELKONTAKTE |  |
| Hardware-Anbieter | Details bereitstellen |
| Eigentümer des Systems | Details bereitstellen |
| Eigentümer der Datenbank | Details bereitstellen |
| Eigentümer der Anwendung | Details bereitstellen |
| Software-Anbieter | Details bereitstellen |
| Offsite-Speicherung | Details bereitstellen |
| Netzdienste | Details bereitstellen |

|  |  |
| --- | --- |
| BACKUP-STRATEGIE für SYSTEM ZWEI |  |
| Täglich | Details bereitstellen |
| Monatlich | Details bereitstellen |
| Vierteljährlich | Details bereitstellen |

|  |  |
| --- | --- |
| **SYSTEM ZWEI** **VERFAHREN FÜR DAS DISASTER RECOVERY** |  |
| Szenario 1  Totalverlust des Schalters | Details bereitstellen |
| Szenario 2  Totalverlust des Netzes | Details bereitstellen |

**ADDENDUM**

|  |  |
| --- | --- |
| **KONTAKTE** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Unterstützungssysteme <Datum>**

|  |  |
| --- | --- |
| Unterstützungssystem | <Details bereitstellen> |
| Kritische Netzwerte | <Details bereitstellen> |
| Kritische Schnittstellen | <Details bereitstellen> |
| Wiederherzustellende kritische Dateien | <Details bereitstellen> |
| Wiederherstellung kritischer Netzwerkdienste | <Details bereitstellen> |
| Sonstige Dienstleistungen | <Details bereitstellen> |

# **Anhang B - Vorgeschlagene Formulare**

## **Formular zur Schadensbewertung**

|  |  |  |
| --- | --- | --- |
| **Wichtigstes Geschäft**  **Betroffener Prozess** | **Beschreibung des Problems** | **Ausmaß der Beschädigung** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Formular Management von DR-Aktivitäten**

* Während des Wiederherstellungsprozesses nach einer Katastrophe werden alle Aktivitäten anhand einer Standardstruktur festgelegt.
* Wenn möglich, muss dieser Plan während des gesamten Zeitraums des Disaster Recoverys in regelmäßigen Abständen aktualisiert werden.
* Alle Aktionen, die in dieser Phase stattfinden, müssen aufgezeichnet werden.

|  |
| --- |
| **Name der Aktivität:** |
| **Referenznummer:** |
| **Kurzbeschreibung:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Beginn**  **Datum/Uhrzeit** | **Fertigstellung**  **Datum/Uhrzeit** | **Involvierte Ressourcen** | **Verantwortlich** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 

## **Formular zur Aufzeichnung von Disaster-Recovery-Ereignissen**

* Alle wichtigen Ereignisse, die während der DR-Phase eintreten, müssen aufgezeichnet werden.
* Der Leiter des DR-Teams muss ein Ereignisprotokoll führen.
* Dieses Ereignisprotokoll sollte bei Eintreten des Notfalls begonnen und eine Kopie des Protokolls an das Business-Reovery-Team weitergeleitet werden, sobald die ersten Gefahren unter Kontrolle sind.
* Das folgende Ereignisprotokoll sollte vom Leiter des DR-Teams ausgefüllt werden, um alle wichtigen Ereignisse während des Disaster Recoverys festzuhalten, bis die Verantwortung an das Business Recovery Team übergeben wird.

|  |
| --- |
| **Beschreibung der Katastrophe:** |
| **Datum des Beginns:** |
| **Datum/Uhrzeit der Mobilisierung des DR-Teams:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Vom DR-Team unternommene Aktivitäten** | **Datum und Uhrzeit** | **Ergebnis** | **Folgemaßnahmen erforderlich** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **Abgeschlossene Arbeiten des Disaster Recovery Teams:** <Datum> |
| **Ereignisprotokoll an das Business Recovery Team weitergeleitet:** <Datum> |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Formular für den Bericht über Disaster-Recovery-Aktivitäten**

* Nach Abschluss der ersten DR-Maßnahmen sollte der DR-Teamleiter einen Bericht über durchgeführten Aktivitäten erstellen.
* Der Bericht sollte Informationen über den Notfall, die benachrichtigten Personen und den Zeitpunkt der Benachrichtigung, die von den Mitgliedern des DR-Teams ergriffenen Maßnahmen sowie die Ergebnisse dieser Maßnahmen enthalten.
* Der Bericht wird auch eine Bewertung der Auswirkungen auf den normalen Geschäftsbetrieb enthalten.
* Der Bericht sollte dem Leiter des Business-Recovery-Teams übergeben werden, mit einer Kopie an die Geschäftsleitung, falls erforderlich.
* Der DR-Teamleiter erstellt nach Abschluss der ersten DR-Maßnahmen einen Bericht.
* Der Bericht wird nicht nur an den Leiter des Business-Recovery-Teams, sondern auch an die Unternehmensleitung verteilt.

Der Bericht wird Folgendes enthalten

* Eine Beschreibung des Notfalls oder Vorfalls
* Personen, die über den Notfall informiert wurden (einschließlich Datum)
* Von Mitgliedern des DR-Teams ergriffene Maßnahmen
* Ergebnisse der durchgeführten Maßnahmen
* Eine Bewertung der Auswirkungen auf den normalen Geschäftsbetrieb
* Bewertung der Wirksamkeit des BCP und der daraus gezogenen Lehren
* Gelernte Lektionen

**\_\_\_\_\_\_\_\_\_\_**

## **Formular für die Mobilisierung des Disaster-Recovery-Teams**

* Nach einem Notfall, der die Wiederherstellung der technischen Infrastruktur erfordert, sollte das Disaster-Recovery-Team über die Situation informiert und in Bereitschaft versetzt werden.
* Das unten abgebildete Format kann für die Aufzeichnung der Aktivierung des DR-Teams verwendet werden, sobald die Arbeit der Schadensbeurteilungs- und ER-Teams abgeschlossen ist.

|  |
| --- |
| **Beschreibung des Notfalls:** |
| Datum des Auftretens: |
| Datum des Abschlusses der Arbeit des Disaster Recovery Teams: |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name des Teammitglieds** | **Kontakt Details** | **Kontaktiert am (Uhrzeit/Datum)** | **Von wem** | **Antwort** | **Erforderliches Startdatum** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Einschlägige Kommentare (z. B. erteilte spezifische Anweisungen) | | | | | |

**\_\_\_\_\_\_\_\_\_\_\_**

## **Formular für die Mobilisierung des Business-Recovery-Teams**

* Nach einem Notfall, der die Aktivierung des Disaster-Recovery-Teams erfordert, sollte das Business-Recovery-Team über die Situation informiert werden und in Bereitschaft versetzt werden.
* Das nachstehende Format wird für die Aufzeichnung der Aktivierung des BR-Teams verwendet, sobald die Arbeit des DR-Teams abgeschlossen ist.

|  |
| --- |
| **Beschreibung des Notfalls:** |
| Datum des Auftretens: |
| Datum des Abschlusses der Arbeit des Business Recovery Teams: |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name des Teammitglieds** | **Kontakt Details** | **Kontaktiert am (Uhrzeit/Datum)** | **Von wem** | **Antwort** | **Erforderliches Startdatum** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Einschlägige Kommentare (zum Beispiel erteilte spezifische Anweisungen) | | | | | |

**\_\_\_\_\_\_\_\_\_\_\_\_**

## **Formular zur Überwachung des Fortschritts von Business-Recovery-Aufgaben**

* Während dieser Zeit muss der Fortschritt der Technologie und der BR-Aufgaben genau überwacht werden.
* Da sich die Schwierigkeiten einer Gruppe erheblich auf andere, abhängige Aufgaben auswirken können, muss sichergestellt werden, dass für jede Aufgabe angemessene Mittel zur Verfügung stehen und dass die zur Wiederherstellung des normalen Geschäftsbetriebs erforderlichen Anstrengungen nicht unterschätzt werden.

*Hinweis: Es muss eine Prioritätsreihenfolge festgelegt werden, obwohl die Aktivitäten, wenn möglich, gleichzeitig durchgeführt werden sollen.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Aufgaben zur Wiederherstellung  (*Reihenfolge der Prioritäten)* | Verantwortliche Person(en) | Datum der Fertigstellung | | Identifizierte Meilensteine | Andere relevante Informationen |
| Geschätzte | Aktuell |
| 1. |  |  |  |  |  |
| 2. |  |  |  |  |  |
| 3. |  |  |  |  |  |
| 4. |  |  |  |  |  |
| 5. |  |  |  |  |  |
| 6. |  |  |  |  |  |
| 7. |  |  |  |  |  |
|  |  |  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_

## **Vorbereitung des Business-Recovery-Report-Formulars**

* Nach Abschluss der Wiederherstellungsmaßnahmen sollte der BRT-Leiter einen Bericht über die durchgeführten und abgeschlossenen Maßnahmen erstellen.
* Der Bericht sollte Informationen über das störende Ereignis, die Personen, die benachrichtigt wurden, und die von den Mitgliedern des BRT ergriffenen Maßnahmen sowie die sich daraus ergebenden Ergebnisse enthalten.
* Der Bericht wird auch eine Bewertung der Auswirkungen auf den normalen Geschäftsbetrieb enthalten.
* Der Bericht sollte gegebenenfalls an die Geschäftsleitung weitergeleitet werden.

Der Inhalt des Berichts muss Folgendes umfassen:

* Eine Beschreibung des Vorfalls
* Personen, die über den Notfall informiert wurden (einschließlich Datum)
* Maßnahmen des Business Recovery Teams
* Ergebnisse der durchgeführten Maßnahmen
* Eine Bewertung der Auswirkungen auf den normalen Geschäftsbetrieb
* Ermittelte Probleme
* Vorschläge zur Verbesserung des Disaster-Recovery- und/oder Business-Continuity-Plans
* Gelernte Lektionen

## **Kommunikationsformular**

* Es ist sehr wichtig, dass alle betroffenen Personen und Organisationen während der Wiederherstellungsmaßnahmen (DR und BR) nach einem Störfall angemessen informiert werden.
* Die Informationen, die an alle Beteiligten weitergegeben werden, müssen korrekt und rechtzeitig sein.
* Insbesondere sollte jede Schätzung des Zeitplans für die Rückkehr zum normalen Arbeitsbetrieb mit Vorsicht verkündet werden.
* Es ist auch sehr wichtig, dass nur befugtes Personal mit Medienabfragen arbeitet

|  |  |  |  |
| --- | --- | --- | --- |
| Gruppen von Personen oder Organisationen, die von der Unterbrechung betroffen sind | Ausgewählte Personen zur Koordinierung der Kommunikation  an betroffene Personen/Organisationen | | |
| Name | Position | Kontakt Details |
| Kunden |  |  |  |
| Management und Personal |  |  |  |
| Anbieter |  |  |  |
| Medien |  |  |  |
| Interessierte Kreise |  |  |  |
| Andere |  |  |  |

**\_\_\_\_\_\_\_\_\_\_\_\_**

## **Rückführung wiederhergestellter Geschäftsabläufe in die Führung der Geschäftseinheit**

* Sobald der normale Geschäftsbetrieb wiederhergestellt ist, muss die Verantwortung für bestimmte Vorgänge wieder an den zuständigen Leiter der Geschäftseinheit zurückgegeben werden.
* Dieser Prozess sollte formalisiert werden, um zu gewährleisten, dass alle Beteiligten die Änderung der Gesamtverantwortung und den Übergang zum *Business-as-usual* verstehen.
* Es ist wahrscheinlich, dass während des Wiederherstellungsprozesses die Gesamtverantwortung an den Leiter des Business-Recovery-Teams übertragen wurde.
* Es wird davon ausgegangen, dass die Geschäftsbereichsleitung während des gesamten Wiederherstellungsprozesses voll involviert ist. Damit der Wiederherstellungsprozess jedoch voll wirksam ist, sollte die Gesamtverantwortung während des Wiederherstellungszeitraums wahrscheinlich bei einem Team für den Geschäftswiederherstellungsprozess (Business Recovery) liegen.

**\_\_\_\_\_\_\_\_\_\_\_\_**

## 

## **Formular für den Abschluss des Geschäftsprozess-/Funktions-Recovery**

Das folgende Übergangsformular sollte für jeden wiederhergestellten Prozess ausgefüllt und vom Leiter des Wiederherstellungsteams und dem verantwortlichen Leiter der Geschäftseinheit unterzeichnet werden.

Für jeden wiederhergestellten Geschäftsprozess sollte ein eigenes Formular verwendet werden.

|  |  |
| --- | --- |
| **Name des Geschäftsprozesses** | |
| **Datum des Abschlusses der vom Business Recovery Team geleisteten Arbeit** |  |
| **Datum des Übergangs zurück zum Business Unit Management**  *(Falls abweichend vom Fertigstellungsdatum)* |  |
| Ich bestätige, dass die Arbeit des Wiederherstellungsteams im Einklang mit dem Notfallplan für den oben genannten Prozess abgeschlossen wurde und dass der normale Geschäftsbetrieb tatsächlich wiederhergestellt wurde.  Business Recovery Team Leader Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Alle relevanten Kommentare des BRT-Leiters im Zusammenhang mit der Rückgabe dieses Geschäftsprozesses sollten hier gemacht werden).* | |
| Ich bestätige, dass der oben beschriebene Geschäftsprozess nun für normale Arbeitsbedingungen akzeptabel ist.  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Titel: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |