IBM Systems - iSeries

# Systemverwaltung
# Planung einer Sicherungs- und Wiederherstellungsstrategie

*Version 5 Release 4*

IBM Systems - iSeries

# Systemverwaltung
# Planung einer Sicherungs- und Wiederherstellungsstrategie

*Version 5 Release 4*

**Hinweis:**
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts lesen Sie die Informationen in „Bemerkungen", auf Seite 21.

**Siebte Ausgabe (Februar 2006)**

Diese Ausgabe bezieht sich auf Version 5, Release 4, Modifikation 0 von IBM i5/OS (Produktnummer 5722-SS1) und auf alle nachfolgenden Releases und Modifikationen, sofern in neuen Ausgaben nicht anders angegeben. Diese Version läuft nicht auf CISC-Modellen und nicht auf allen RISC-Modellen (RISC - reduced instruction set computer).

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
*IBM Systems - iSeries System Administration Plan a backup and recovery strategy, Version 5 Release 4,*
herausgegeben von International Business Machines Corporation, USA



Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2006

# Inhaltsverzeichnis

# Planung einer Sicherungs- und Wiederherstellungsstrategie

Dieses Thema beschreibt die Vorgehensweise, wenn bei Verlust von Informationen auf Ihrem System Sicherungskopien verwendet werden müssen.

Computer sind im Allgemeinen sehr zuverlässig, ganz besonders gilt dies für den IBM eServer iSeries-Server. Sie können Ihr System monate- oder sogar jahrelang einsetzen, ohne dass Störungen auftreten, die zum Datenverlust auf Ihrem System führen. In demselben Maße wie die Häufigkeit von Problemen abgenommen hat, haben die potenziellen Auswirkungen von Problemen jedoch ein kritisches Maß angenommen. Unternehmen sind immer mehr von Computern und den darauf gespeicherten Informationen abhängig. Die Informationen, die sich auf Ihrem Computer befinden, sind möglicherweise an keiner anderen Stelle verfügbar.

Die Datensicherung auf Ihrem System ist zeitaufwendig und erfordert Disziplin. Warum also sollten Sie eine Datensicherung durchführen? Warum Zeit für die Planung und Bewertung der Datensicherung aufwenden?

Die Antwort ist einfach: Weil sonst unter Umständen Probleme auf Sie zukommen. Sie werden irgendwann auf Sicherungskopien Ihrer Daten zurückgreifen müssen, da bei jedem System früher oder später, aus welchen Gründen auch immer, die gesamten Daten oder Teile davon zurückgespeichert werden müssen.

Der Zeitrahmen für die Sicherung und Wiederherstellung stellt eine Übersicht der oberen Ebene über die Ereignisse bereit, die während des Sicherungs- und Wiederherstellungsprozesses auftreten.

Nachdem Sie den Zeitrahmen für die Sicherung und Wiederherstellung studiert haben, können Sie mit dem Planen Ihrer Strategie beginnen. Führen Sie folgende Schritte aus:

1. Zu sichernde Daten und Häufigkeit der Sicherungen festlegen.
2. Sicherungsfenster bestimmen.
3. Verfügbarkeitsoptionen auswählen.
4. Strategie testen.

Das Thema ″Wiederherstellung nach einem Katastrophenfall planen″ kann auch als Planungsressource hilfreich sein.

Dieses Thema enthält Informationen zum Planen einer Strategie und zu den Auswahlen, die Sie beim Konfigurieren Ihres Systems hinsichtlich der Sicherung, Wiederherstellung und Verfügbarkeit treffen müssen. Informationen zur Ausführung der Tasks, die sich auf diese Themen beziehen, befinden sich im

Handbuch Sicherung und Wiederherstellung  sowie unter dem Thema ″Server sichern″. Die Roadmap zur Verfügbarkeit stellt Informationen zu den allgemeinen Arten von Fehlern zur Verfügung, die auftreten können.

**Zugehörige Konzepte**

Server sichern

Roadmap zur Verfügbarkeit für Ihren iSeries-Server

## Druckbare PDF

Verwenden Sie diese Angaben, um eine PDF mit diesen Informationen anzuzeigen und zu drucken.

Um die PDF-Version dieses Dokuments anzuzeigen oder herunterzuladen, wählen Sie Planung einer Sicherungs- und Wiederherstellungsstrategie aus (ca. 317 KB).

### PDF-Dateien sichern

Gehen Sie wie folgt vor, um eine PDF zum Anzeigen oder Drucken auf Ihrer Workstation zu sichern:

1. Klicken Sie in Ihrem Browser mit der rechten Maustaste auf die PDF (klicken Sie mit der rechten Maustaste auf den Link weiter oben).
2. Klicken Sie auf die Option, mit der die PDF lokal gesichert wird.
3. Navigieren Sie zu dem Verzeichnis, in dem die PDF gesichert werden soll.
4. Klicken Sie auf **Sichern**.

### Adobe Reader herunterladen

Adobe Reader muss auf Ihrem System installiert sein, um diese PDFs anzuzeigen oder zu drucken. Sie können eine kostenlose Kopie von der Adobe-Website (www.adobe.com/products/acrobat/readstep.html)  herunterladen.

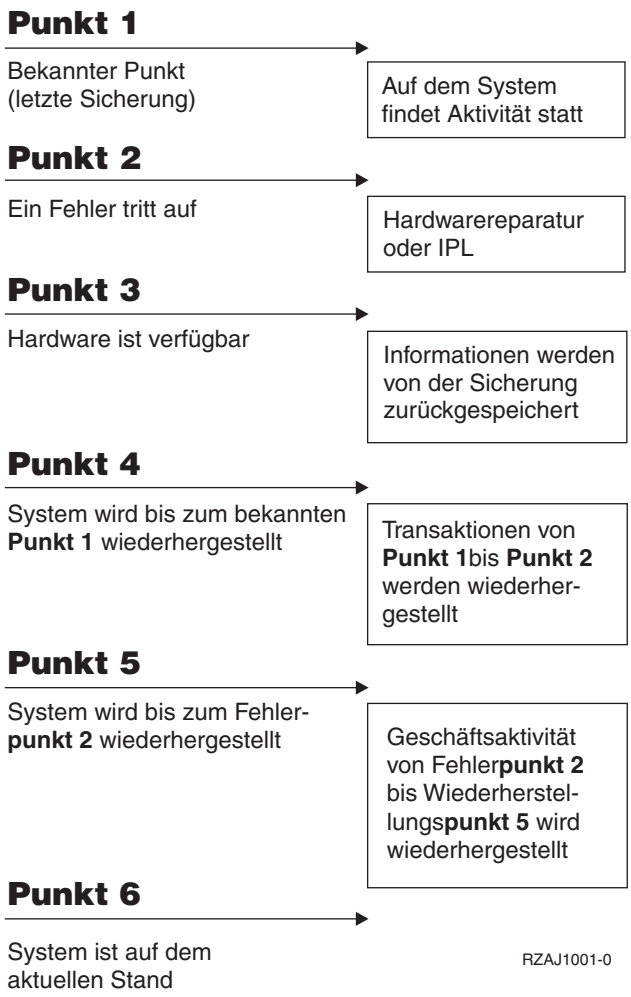
## Zeitrahmen für Sicherung und Wiederherstellung

Der Zeitrahmen für die Sicherung und Wiederherstellung beginnt, wenn Sie Informationen sichern, und endet, wenn Ihr System nach einem Ausfall vollständig wiederhergestellt wurde.

Berücksichtigen Sie diesen Zeitrahmen, wenn Sie die nachfolgenden Informationen lesen und Entscheidungen treffen. Ihre Strategie für die Sicherung und Verfügbarkeit legt Folgendes fest:

- Ob Sie jeden Schritt im Diagramm erfolgreich ausführen können
- Wie lange Sie für die Ausführung jedes Schritts benötigen

Verwenden Sie den folgenden Zeitrahmen, um spezielle Beispiele zu erstellen. Was wäre, wenn der bekannte Punkt (1) ein Sonntagabend und der Fehlerpunkt (2) ein Donnerstag Nachmittag ist? Wie lange dauert es, zum bekannten Punkt zurückzukehren? Wie lange dauert es, zum aktuellen Punkt (6) zu gelangen? Ist dies mit der von Ihnen geplanten Sicherungsstrategie überhaupt möglich?




Es folgt eine Beschreibung der Grafik mit dem Zeitrahmen:

- Punkt 1: Bekannter Punkt (letzte Sicherung). Auf dem System findet Aktivität statt.
- Punkt 2: Ein Fehler tritt auf. Hardwarereparatur oder IPL (Initial Program Load = Einleitendes Programmladen) wird durchgeführt.
- Punkt 3: Hardware ist verfügbar. Die Daten werden von der Sicherung zurückgespeichert.
- Punkt 4: Das System wird beim bekannten Punkt 1 wiederhergestellt. Transaktionen von Punkt 1 bis Punkt 2 werden wiederhergestellt.
- Punkt 5: Das System wird beim Fehlerpunkt 2 wiederhergestellt. Geschäftsaktivität von Fehlerpunkt 2 bis Wiederherstellungspunkt 5 wird wiederhergestellt.
- Punkt 6: Das System ist auf dem aktuellen Stand.

**Zugehörige Konzepte**

„Strategie testen" auf Seite 9
Wenn für Ihre Anforderungen eine mittlere Sicherungsstrategie oder eine komplexe Sicherungsstrategie benötigt wird, muss regelmäßig eine Überprüfung durchgeführt werden.

**Zugehörige Verweise**

„Zu sichernde Daten und Häufigkeit der Sicherungen festlegen"
Sie sollten alle Daten in Ihrem System so oft wie möglich sichern.

## Zu sichernde Daten und Häufigkeit der Sicherungen festlegen

Sie sollten alle Daten in Ihrem System so oft wie möglich sichern.

Wenn Sie nicht regelmäßig alle Daten sichern, können Sie bei einem Standortverlust oder bei bestimmten Arten von Plattenfehlern unter Umständen keine Wiederherstellung durchführen.

Wenn Sie die entsprechenden Teile Ihres iSeries-Servers sichern, können Sie die Wiederherstellung bis zum Punkt 4 (letzte Sicherung), der beim Zeitrahmen für Sicherung und Wiederherstellung gezeigt wird, durchführen. Teile des Systems, die häufigen Änderungen unterliegen, sollten Sie täglich sichern.

Alle anderen Teile sollten wöchentlich gesichert werden.

## Teile des Systems, die häufigen Änderungen unterliegen

Die nachfolgende Tabelle zeigt die Teile des Systems, die sich oft ändern und deshalb täglich gesichert werden sollten.

*Tabelle 1. Teile, die täglich gesichert werden sollten*

| Beschreibung des Systembestandteils | Von IBM geliefert? | Wann Änderungen auftreten |
|---|---|---|
| Sicherheitsinformationen (Benutzerprofile, persönliche Berechtigungen, Berechtigungslisten) | Einige | Regelmäßig, wenn neue Benutzer und Objekte hinzugefügt werden oder Berechtigungen sich ändern[1] |
| Konfigurationsobjekte in QSYS | Nein | Regelmäßig, wenn Einheitenbeschreibungen hinzugefügt oder geändert werden oder wenn Sie die Funktion Hardware Service Manager verwenden, um Konfigurationsdaten zu aktualisieren[1] |
| Von IBM gelieferte Bibliotheken, die Benutzerdaten enthalten (QGPL, QUSRSYS) | Ja | Regelmäßig |
| Benutzerbibliotheken, die Benutzerdaten und Programme enthalten | Nein | Regelmäßig |
| Ordner und Dokumente | Einige | Regelmäßig, wenn Sie diese Objekte verwenden |
| Verteilungsoperationen | Nein | Regelmäßig, wenn Sie die Verteilungsfunktion verwenden |
| Benutzerverzeichnisse | Nein | Regelmäßig |

[1] Diese Objekte können sich auch ändern, wenn Sie lizenzierte Programme aktualisieren.

## Teile des Systems, die sich nicht oft ändern

Die nachfolgende Tabelle zeigt die Teile des Systems, die sich nicht oft ändern und deshalb auf wöchentlicher Basis gesichert werden können.

*Tabelle 2. Teile, die wöchentlich gesichert werden sollten*

| Beschreibung des Systembestandteils | Von IBM geliefert? | Wann Änderungen auftreten |
|---|---|---|
| lizenzierter interner Code (LIC) | Ja | Vorläufige Programmkorrekturen (PTFs) oder ein neues Release des Betriebssystems |
| Betriebssystemobjekte in der Bibliothek QSYS | Ja | PTFs oder ein neues Release des Betriebssystems |
| Optionale Bibliotheken von IBM i5/OS (QHLPSYS, QUSRTOOL) | Ja | PTFs oder ein neues Release des Betriebssystems |
| Lizenzprogrammbibliotheken (QRPG, QCBL, Qxxxx) | Ja | Änderungen an Lizenzprogrammen |
| Lizenzprogrammordner (Qxxxxxxx) | Ja | Änderungen an Lizenzprogrammen |
| Lizenzprogrammverzeichnisse (/QIBM/ProdData, /QOpenSys/QIBM/ProdData) | Ja | Änderungen an Lizenzprogrammen |

**Zugehörige Konzepte**

„Zeitrahmen für Sicherung und Wiederherstellung" auf Seite 2
Der Zeitrahmen für die Sicherung und Wiederherstellung beginnt, wenn Sie Informationen sichern, und endet, wenn Ihr System nach einem Ausfall vollständig wiederhergestellt wurde.

**Zugehörige Verweise**

„Einfache Sicherungsstrategie"
Ihnen steht täglich ein ausgedehntes Sicherungsfenster mit acht bis zwölf Stunden zur Verfügung, in dem keine Systemaktivität stattfindet (einschließlich Stapelbetrieb). Die einfachste Sicherungsstrategie besteht darin, alle Daten jede Nacht oder außerhalb der Betriebszeiten zu sichern.

## Sicherungsfenster bestimmen

Bei der Ausführung von Sicherungsprozeduren ist die Größe Ihres Sicherungsfensters dafür entscheidend, wie Sie Sicherungsprozeduren ausführen und welche Daten Sie sichern.

Unter dem **Sicherungsfenster** versteht man die Zeitspanne, in der Ihr System nicht für Benutzer zur Verfügung steht, da Sie Sicherungsoperationen ausführen. Zur Vereinfachung der Wiederherstellung müssen Sie zu dem Zeitpunkt sichern, wenn sich das System an einem bekannten Punkt befindet und sich die Daten nicht ändern. Bei der Auswahl einer Sicherungsstrategie müssen Sie die Systemverfügbarkeit für die Benutzer (d. h. welches Sicherungsfenster für die Benutzer akzeptabel ist) gegen den Wert der Daten, die unter Umständen verloren gehen, und den Zeitaufwand für die Wiederherstellung abwägen.

Wenn Ihr System so kritisch für Ihr Unternehmen ist, dass Sie über kein akzeptables Sicherungsfenster verfügen, können Sie sich wahrscheinlich auch keinen unvorhergesehenen Systemausfall leisten. In diesem Fall sollten Sie ernsthaft alle Verfügbarkeitsoptionen des iSeries-Servers, einschließlich Cluster, einer Bewertung unterziehen. Das Thema "Roadmap zur Verfügbarkeit für Ihren iSeries-Server" enthält weitere Informationen zu Verfügbarkeitsoptionen.

Wählen Sie auf der Basis der Größe Ihres Sicherungsfensters eine der folgenden Sicherungsstrategien aus: einfache, mittlere oder komplexe Sicherungsstrategie. Bewerten Sie dann Ihre Entscheidung im Hinblick darauf, welche Möglichkeiten Ihnen die Sicherungsstrategie für eine Wiederherstellung bietet, nochmals neu.

**Zugehörige Konzepte**

Roadmap zur Verfügbarkeit für Ihren iSeries-Server

## Einfache Sicherungsstrategie

Ihnen steht täglich ein ausgedehntes Sicherungsfenster mit acht bis zwölf Stunden zur Verfügung, in dem keine Systemaktivität stattfindet (einschließlich Stapelbetrieb). Die einfachste Sicherungsstrategie besteht darin, alle Daten jede Nacht oder außerhalb der Betriebszeiten zu sichern.

Dazu können Sie mit Option 21 (Gesamtes System) im Menü SICHERN arbeiten. Sie können Option 21 so terminieren, dass die Sicherung ohne Bedienereingriff (nichtüberwacht) zu einem bestimmten Zeitpunkt ausgeführt wird.

Sie können diese Methode auch für die Sicherung Ihres gesamten Systems nach einem Upgrade auf ein neues Release oder nach dem Installieren von vorläufigen Programmkorrekturen (PTFs) verwenden.

Möglicherweise stellen Sie fest, dass Ihnen nicht genügend Zeit zur Verfügung steht bzw. nicht genügend Bandeinheiten vorhanden sind, um Option 21 ohne einen Bediener auszuführen. In diesem Fall können Sie dennoch eine einfache Strategie verfolgen:

| | |
|---|---|
| Täglich | Alle Daten sichern, die sich oft ändern. |
| Wöchentlich | Alle Daten sichern, die sich nicht oft ändern. |

Option 23 (Alle Benutzerdaten) im Menü SICHERN sichert die Daten, die regelmäßig geändert werden. Option 23 kann so terminiert werden, dass sie nichtüberwacht ausgeführt wird. Dazu müssen allerdings genügend Online-Sicherungsdatenträger zur Verfügung stehen.

Wenn Ihr System an Wochenenden längere Zeit nicht benutzt wird, könnte Ihre Sicherungsstrategie wie folgt aussehen:

| | |
|---|---|
| Freitagnacht | Menü SICHERN, Option 21 |
| Montagnacht | Menü SICHERN, Option 23 |
| Dienstagnacht | Menü SICHERN, Option 23 |
| Mittwochnacht | Menü SICHERN, Option 23 |
| Donnerstagnacht | Menü SICHERN, Option 23 |
| Freitagnacht | Menü SICHERN, Option 21 |

**Zugehörige Verweise**

„Zu sichernde Daten und Häufigkeit der Sicherungen festlegen" auf Seite 3
Sie sollten alle Daten in Ihrem System so oft wie möglich sichern.

## Mittlere Sicherungsstrategie

Sie haben ein mittleres Sicherungsfenster, d. h., Ihnen steht täglich ein 4- bis 6-stündiger Zeitblock zur Verfügung, in dem keine Systemaktivität stattfindet. Verwenden Sie diese Strategie, wenn Sie feststellen, dass Ihr Sicherungsfenster nicht groß genug ist, um eine einfache Sicherungsstrategie zu verfolgen.

Gründe dafür können umfangreiche Stapeljobs sein, die nachts ausgeführt werden müssen. Oder Sie haben sehr große Dateien, für deren Sicherung viel Zeit benötigt wird. Wenn dies der Fall ist, müssen Sie unter Umständen eine mittlere Sicherungsstrategie entwickeln, d. h., für die Sicherung und Wiederherstellung muss ein Mittelweg gewählt werden.

Beim Entwickeln einer mittleren Sicherungsstrategie sollten Sie nach folgendem Prinzip vorgehen: Je öfter Daten geändert werden, desto öfter sollten sie gesichert werden. Sie müssen bei der Auswertung der Häufigkeit von Datenänderungen mehr ins Detail gehen als bei einer einfachen Strategie.

Für eine mittlere Sicherungsstrategie stehen mehrere Methoden zur Verfügung. Sie können eine Methode oder eine Kombination aus verschiedenen Methoden verwenden:
- Geänderte Objekte sichern.
- Objekte aufzeichnen und die Journalempfänger sichern.

### Geänderte Objekte sichern

Sie können mit mehreren Befehlen arbeiten, um nur die Informationen zu sichern, die seit der letzten Sicherungsoperation bzw. seit einem bestimmten Datum und einer bestimmten Uhrzeit geändert wurden.

Mit dem Befehl SAVCHGOBJ (Save Changed Objects - Geänderte Objekte sichern) können Sie nur die Objekte sichern, die seit der letzten Sicherung einer Bibliothek oder einer Gruppe von Bibliotheken geändert wurden. Dies kann besonders dann hilfreich sein, wenn sich Programme und Datendateien in derselben Bibliothek befinden. In der Regel werden Datendateien häufig und Programme seltener geändert. Der Befehl SAVCHGOBJ erlaubt es Ihnen, lediglich die Dateien zu sichern, die geändert wurden.

Der Befehl SAVDLO (Save Document Library Object - Dokumentbibliotheksobjekt sichern) ermöglicht es, nur Dokumente und Ordner zu sichern, die sich geändert haben. Analog können Sie mit dem Befehl SAV (Save- Sichern) Objekte in Verzeichnissen sichern, die sich seit einem bestimmten Zeitpunkt geändert haben.

Sie könnten sich auch für das Sichern von geänderten Objekten entscheiden, wenn die Stapelauslastung in manchen Nächten größer als gewöhnlich ist. Beispiel:

| Tag | Stapelauslastung | Sicherungsoperation |
|---|---|---|
| Freitagnacht | Gering | Menü SICHERN, Option 21 |
| Montagnacht | Groß | Nur Änderungen sichern[1] |
| Dienstagnacht | Gering | Menü SICHERN, Option 23 |
| Mittwochnacht | Groß | Nur Änderungen sichern[1] |
| Donnerstagnacht | Groß | Nur Änderungen sichern[1] |
| Freitagnacht | Gering | Menü SICHERN, Option 21 |

[1] Verwenden Sie eine Kombination aus den Befehlen SAVCHGOBJ, SAVDLO und SAV.

## Objekte aufzeichnen und Journalempfänger sichern

Wenn die Sicherungsoperationen für Datenbankdateien zu lange dauern, da die Dateien umfangreich sind, hilft es Ihnen nicht, geänderte Objekte zu sichern.

Wenn Sie eine Teildatei mit 100.000 Sätzen haben und sich 1 Satz ändert, sichert der Befehl SAVCHGOBJ die gesamte Teildatei. In diesem Fall stellt das Aufzeichnen Ihrer Datenbankdateien und das regelmäßige Sichern der Journalempfänger unter Umständen eine bessere Lösung dar, selbst wenn sich die Wiederherstellung komplexer gestaltet.

Ein ähnliches Prinzip gilt bei IFS-Objekten und -Datenbereichen (IFS - Integrated File System). Wenn Ihre Sicherungsoperationen für IFS-Objekte und -Datenbereiche zu lange dauern, können Sie die Objekte aufzeichnen und die Sicherungsoperationen effizienter gestalten. Das Sichern von Journalempfänger ist unter Umständen die bessere Option.

Beim Aufzeichnen von Objekten schreibt das System eine Kopie jeder Objektänderung in einen Journalempfänger. Wenn Sie einen Journalempfänger sichern, werden lediglich die geänderten Teile des Objekts gesichert, nicht das gesamte Objekt.

Wenn Sie Objekte aufzeichnen und die Stapelauslastung variiert, könnte Ihre Sicherungsstrategie wie folgt aussehen:

*Tabelle 3. Beispiel für Sicherungsstrategie*

| Tag | Stapelauslastung | Sicherungsoperation |
|---|---|---|
| Freitagnacht | Gering | Menü SICHERN, Option 21 |
| Montagnacht | Groß | Journalempfänger sichern |
| Dienstagnacht | Gering | Menü SICHERN, Option 23 |
| Mittwochnacht | Groß | Journalempfänger sichern |
| Donnerstagnacht | Groß | Journalempfänger sichern |
| Freitagnacht | Gering | Menü SICHERN, Option 21 |

**Anmerkungen:**

1. Um sich den Schutz, den die Aufzeichnung bietet, zunutze zu machen, sollten Sie die Journalempfänger regelmäßig abhängen und sichern. Wie oft sie gesichert werden sollten, hängt von der Anzahl der aufgezeichneten Änderungen ab. Möglicherweise ist es in Ihrem Fall angebracht, Journalempfänger mehrmals am Tag zu sichern. Wie Sie Journalempfänger sichern, hängt davon ab, ob sie sich in einer separaten Bibliothek befinden. Sie könnten den Befehl SAVLIB (Save Library - Bibliothek sichern) oder den Befehl SAVOBJ (Save Object - Objekt sichern) verwenden.
2. Neue Objekte müssen gesichert werden, bevor Journaleinträge für ein Objekt angelegt werden können.

   Wenn Ihre Anwendungen regelmäßig neue Objekte hinzufügen, sollten Sie in Erwägung ziehen, mit dem Befehl SAVCHGOBJ zu arbeiten, entweder allein oder in Kombination mit der Journalführung.

**Zugehörige Konzepte**

Journalverwaltung

## Komplexe Sicherungsstrategie

Sie verfügen nur über ein enges Sicherungsfenster, so dass das System, abgesehen von wenigen Ausnahmen, ständig für interaktive Tätigkeiten oder für den Stapelbetrieb verwendet wird. Steht nur ein sehr enges Sicherungsfenster zur Verfügung, muss für die Sicherung und Wiederherstellung eine komplexe Strategie verfolgt werden.

Sie können dieselben Tools und Methoden verwenden, die im Zusammenhang mit der mittleren Sicherungsstrategie oben beschrieben wurden, aber auf einer höheren Detaillierungsebene. Beispielsweise müssen Sie unter Umständen bestimmte kritische Dateien zu bestimmten Tageszeiten oder an bestimmten Wochentagen sichern. Außerdem soll möglicherweise die Verwendung eines Tools, wie beispielsweise IBM Backup Recovery and Media Services for iSeries (BRMS), in Betracht gezogen werden.

Bei einer komplexen Sicherungsstrategie ist es oft erforderlich, das System zu sichern, während es aktiv ist. Der Parameter SAVACT (save active - Sicherung im aktiven Zustand) wird bei folgenden Befehlen unterstützt:

- SAVLIB (Bibliothek sichern)
- SAVOBJ (Objekt sichern)
- SAVCHGOBJ (Geänderte Objekte sichern)
- SAVDLO (Dokumentbibliotheksobjekt sichern)
- SAV (Sichern)

Wenn Sie mit der Unterstützung für die Sicherung im aktiven Zustand arbeiten, können Sie den Zeitraum, in dem die Dateien nicht zur Verfügung stehen, signifikant reduzieren. Wenn das System für alle Objekte, die gerade gesichert werden, einen Prüfpunkt erstellt hat, stehen die Objekte zwecks weitere Verwendung zur Verfügung. Die Unterstützung für die Sicherung im aktiven Zustand kann in Kombination mit der Journalführung und der COMMIT-Steuerung verwendet werden, um die Wiederherstellungsprozedur zu vereinfachen. Wenn Sie beim Parameter SAVACT die Werte *LIB oder *SYNCLIB verwenden, sollten Sie mit der Journalführung arbeiten, um die Wiederherstellung zu vereinfachen. Wenn Sie beim Parameter SAVACT den Wert *SYSDFN angeben, müssen Sie auch mit COMMIT-Steuerung arbeiten, wenn die zu sichernde Bibliothek zusammengehörige Datenbankobjekte enthält. Wenn Sie die Unterstützung für die Sicherung im aktiven Zustand wählen, müssen Sie unbedingt mit dem Prozedere vertraut sein und überwachen, wie gut Prüfpunkte auf Ihrem System erstellt werden.

Sie können den Zeitraum, in dem Dateien nicht zur Verfügung stehen, ebenfalls reduzieren, indem Sie Sicherungsoperationen auf mehreren Einheiten ausführen oder indem Sie *gleichzeitig ablaufende Sicherungsoperationen* ausführen. Sie können beispielsweise Bibliotheken auf einer Einheit sichern, Ordner auf einer anderen Einheit und Verzeichnisse wiederum auf einer dritten Einheit. Sie können auch unterschiedliche Bibliothekengruppen oder Objektgruppen auf verschiedenen Einheiten sichern.

Außerdem können Sie mehrere Einheiten gleichzeitig verwenden, indem Sie eine *parallele Sicherungsoperation* ausführen. Um eine parallele Sicherungsoperation ausführen zu können, benötigen Sie Backup Recovery and Media Services oder eine Anwendung, mit der Sie Datenträgerdefinitionsobjekte erstellen können.

Weitere Informationen zur Unterstützung für die Sicherung im aktiven Zustand, zu gleichzeitig ablaufenden Sicherungsoperationen und zu parallelen Sicherungsoperationen befinden sich unter dem Thema ″Server sichern″.

**Zugehörige Konzepte**

IBM Backup Recovery and Media Services for iSeries

Im aktiven Zustand

Mehrere Einheiten

Server sichern
COMMIT-Steuerung
Journalverwaltung

## Verfügbarkeitsoptionen auswählen

Verfügbarkeitsoptionen sind kein Ersatz für eine gute Sicherungsstrategie, sondern eine Ergänzung.

Verfügbarkeitsoptionen können die Dauer einer Wiederherstellung nach einem Fehler signifikant verkürzen. In manchen Fällen können Verfügbarkeitsoptionen sogar verhindern, dass Sie eine Wiederherstellung durchführen müssen.

Um die Kosten für den Einsatz von Verfügbarkeitsoptionen zu rechtfertigen, müssen Sie Folgendes berücksichtigen:

- Den Wert, den Ihr System bereitstellt.
- Die Kosten eines terminierten oder nicht terminierten Ausfalls.
- Ihre Verfügbarkeitsanforderungen.

Die folgende Liste zeigt die Verfügbarkeitsoptionen, die Sie verwenden können, um Ihre Sicherungsstrategie zu ergänzen:

- Durch Journalverwaltung können Änderungen an Objekten, die seit der letzten vollständigen Sicherung vorgenommen wurden, wiederhergestellt werden.
- Mit dem Zugriffspfadschutz können Sie die Reihenfolge, in der Sätze in einer Datenbankdatei bearbeitet werden, erneut erstellen.
- Plattenpools beschränken die Datenmenge, die wiederhergestellt werden muss, auf die Daten im Plattenpool der fehlgeschlagenen Einheit.
- Der Einheitenparitätsschutz ermöglicht Ihnen, die verloren gegangenen Daten wiederherzustellen; der Systembetrieb kann fortgesetzt werden, während die Daten wiederhergestellt werden.
- Der Spiegelschutz hilft, die Daten verfügbar zu halten, da Sie über zwei Kopien der Daten auf zwei separaten Platteneinheiten verfügen.
- Beim Clustering können einige oder alle Daten auf zwei Systemen verwaltet werden; das sekundäre System kann kritische Anwendungen übernehmen, wenn im primären System ein Fehler auftritt.

Das Thema "Roadmap zur Verfügbarkeit für Ihre iSeries" enthält Informationen, anhand derer Sie eine Verfügbarkeitslösung auf Ihrem iSeries-Server implementieren können.

**Zugehörige Konzepte**

Roadmap zur Verfügbarkeit für Ihren iSeries-Server

**Zugehörige Verweise**

Sonderwerte für den Befehl SAVLIB

## Strategie testen

Wenn für Ihre Anforderungen eine mittlere Sicherungsstrategie oder eine komplexe Sicherungsstrategie benötigt wird, muss regelmäßig eine Überprüfung durchgeführt werden.

Bei der regelmäßigen Überprüfung ist Folgendes zu berücksichtigen:

- Sichern Sie **alles** von Zeit zu Zeit?
- Was müssen Sie tun, um eine Wiederherstellung zum bekannten Punkt (4) innerhalb des Zeitrahmens für die Sicherung und Wiederherstellung durchzuführen?

- Verwenden Sie Optionen, wie beispielsweise die Journalführung oder das Sichern von geänderten Objekten, um die Wiederherstellung beim Fehlerpunkt (5) zu unterstützen? Sind Sie mit der Vorgehensweise bei der Wiederherstellung unter Verwendung dieser Optionen vertraut?
- Haben Sie neue Anwendungen hinzugefügt? Werden die neuen Bibliotheken, Ordner und Verzeichnisse gesichert?
- Sind die von IBM gelieferten Bibliotheken, die Benutzerdaten enthalten (zum Beispiel QGPL und QUSRSYS), Teil der Sicherung?

  **Anmerkung:** Unter dem Thema Sonderwerte für den Befehl SAVLIB sind alle von IBM gelieferten Bibliotheken, die Benutzerdaten enthalten, aufgelistet.
- Haben Sie die Wiederherstellung getestet?

Der beste Weg, Ihre Strategie zu testen, besteht darin, einen Testlauf für eine Wiederherstellung durchzuführen. Wenn Sie eine Wiederherstellung auf Ihrem eigenen System ausführen, kann dies riskant sein. Wenn Sie nicht alle Daten erfolgreich gesichert haben, gehen bei der versuchten Wiederherstellung möglicherweise Daten verloren.

Eine ganze Reihe von Unternehmen bieten Tests für Wiederherstellungen als Dienstleistung an. IBM Continuity and Recovery Services ist ein solches Unternehmen, das Ihnen bei Wiederherstellungstests behilflich sein kann.

**Zugehörige Konzepte**

„Zeitrahmen für Sicherung und Wiederherstellung" auf Seite 2
Der Zeitrahmen für die Sicherung und Wiederherstellung beginnt, wenn Sie Informationen sichern, und endet, wenn Ihr System nach einem Ausfall vollständig wiederhergestellt wurde.

---

## Wiederherstellung nach einem Katastrophenfall planen

Dieses Thema stellt Richtlinien für die Informationen und Prozeduren zur Verfügung, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind.

Der Zweck eines Plans zur Wiederherstellung nach einem Katastrophenfall ist es, sicherzustellen, dass auf einen Notfall oder auf eine andere Ausnahmesituation, die Informationssysteme beeinträchtigt, reagiert werden kann und die Auswirkungen auf den Geschäftsbetrieb dabei so gering wie möglich gehalten werden. Wenn Sie die in diesem Thema beschriebenen Informationen schriftlich fixiert haben, sollten Sie das Dokument an einem sicheren und zugänglichen Ort außerhalb des Unternehmens aufbewahren.

Nachfolgend finden Sie eine Schablone, die Sie beim Erstellen eines Plans zur Wiederherstellung nach einem Katastrophenfall verwenden können. Sie können diese Schablone hier anzeigen; zum Drucken der Schablone müssen Sie die PDF-Datei für dieses Thema herunterladen und drucken.

## Plan zur Wiederherstellung nach einem Katastrophenfall

Dieses Thema enthält Informationen zur Erstellung eines Plans zur Wiederherstellung nach einem Katastrophenfall.

### Abschnitt 1. Hauptziele dieses Plans

Die Hauptziele dieses Plans sind:

- Unterbrechungen des normalen Geschäftsbetriebs so gering wie möglich halten.
- Das Ausmaß von Unterbrechungen und Beschädigungen begrenzen.
- Die wirtschaftlichen Auswirkungen einer Unterbrechung so gering wie möglich halten.
- Im Voraus alternative Betriebsmöglichkeiten einrichten.
- Das Personal mit den Maßnahmen, die im Notfall zu ergreifen sind, vertraut machen.

- Eine problemlose und schnelle Wiederherstellung des Service ermöglichen.

## Abschnitt 2. Personal

*Tabelle 4. Personal*

| **Datenverarbeitungspersonal** | | | |
|---|---|---|---|
| **Name** | **Position** | **Adresse** | **Telefon** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Anmerkung:** Hängen Sie an diesen Abschnitt des Plans eine Kopie Ihres Organisationsdiagramms an.

## Abschnitt 3. Anwendungsprofil

Verwenden Sie den Befehl DSPSFWRSC (Display Software Resources - Softwareressourcen anzeigen) zum Ausfüllen dieser Tabelle.

*Tabelle 5. Anwendungsprofil*

| **Anwendungsprofil** | | | | |
|---|---|---|---|---|
| **Anwendungsname** | **Kritisch? Ja/Nein** | **Anlagevermögen? Ja/Nein** | **Hersteller** | **Kommentare** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | **Legende für Kommentare:** |
| | | | | 1. Tägliche Ausführung _____. |
| | | | | 2. Wöchentliche Ausführung am _____. |
| | | | | 3. Monatliche Ausführung am _____. |

## Abschnitt 4. Hardwareprofil

Verwenden Sie den Befehl WRKHDWPRD (Work with Hardware Products - Mit Hardwareprodukten arbeiten) zum Ausfüllen dieser Tabelle. Diese Liste sollte Folgendes beinhalten:

- Verarbeitungseinheiten
- Platteneinheiten
- Modelle
- Workstation-Controller
- Personal Computer
- Ersatz-Workstations
- Telefone
- Heizung/Klimaanlage
- Systemdrucker
- Band- und Disketteneinheiten
- Controller
- E/A-Prozessoren
- Allgemeine Datenübertragung
- Ersatzbildschirme
- Gehäuserahmen
- Luftfeuchtigkeitsregler

*Tabelle 6. Hardwareprofil*

| **Hardwareprofil** | | | | | |
|---|---|---|---|---|---|
| **Hersteller** | **Beschreibung** | **Modell** | **Seriennummer** | **Gekauft oder geleast** | **Kosten** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Anmerkung:** Diese Liste sollte alle _____ Monate überprüft werden. | | | | | |

*Tabelle 7. Zubehör (Verschiedenes)*

| **Zubehör (Verschiedenes)** | | |
|---|---|---|
| **Beschreibung** | **Menge** | **Kommentare** |
| | | |
| | | |
| | | |
| | | |
| | | |

*Tabelle 7. Zubehör (Verschiedenes) (Forts.)*

| **Zubehör (Verschiedenes)** | | |
|---|---|---|
| **Beschreibung** | **Menge** | **Kommentare** |
| **Anmerkung:** Diese Liste sollte Folgendes beinhalten:<br>• Bänder<br>• PC-Software (beispielsweise DOS)<br>• Akten oder Dokumentation<br>• Bänder im Sicherheitsraum<br>• Disketten<br>• Emulationspakete<br>• Programmiersprachensoftware (wie COBOL und RPG)<br>• Druckerzubehör (wie Papier und Formulare) | | |

## Abschnitt 5. Sicherungsprozeduren für Informationsservices

- iSeries-Server
  - Journalempfänger werden täglich um _____ Uhr und um _____ Uhr geändert.
  - Geänderte Objekte in folgenden Bibliotheken und Verzeichnissen werden täglich um _____ Uhr gesichert:
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    Mit dieser Prozedur werden auch die Journale und Journalempfänger gesichert.
  - Am _____ (Tag) um _____ (Uhrzeit) wird eine vollständige Sicherung des Systems ausgeführt.
  - Alle Sicherungsdatenträger werden außerhalb des Unternehmens in einem Sicherheitsraum in _____ (Standort) aufbewahrt.
- Personal Computer
  - Es wird empfohlen, die Daten auf allen Personal Computern zu sichern. Kopien der PC-Dateien sollten unmittelbar vor der vollständigen Sicherung des Systems am _____ (Datum) um _____ (Uhrzeit) auf den Server hochgeladen werden. Das System wird dann mit der normalen Systemsicherungsprozedur gesichert. Auf diese Weise wird eine zuverlässigere Sicherung von PC-bezogenen Systemen erreicht, bei denen durch einen lokalen Notfall Daten wichtiger PC-Systeme gelöscht werden können.

## Abschnitt 6. Prozeduren zur Wiederherstellung nach einem Katastrophenfall

Bei jedem Plan für die Wiederherstellung nach einem Katastrophenfall sollten die drei folgenden Bereiche abgedeckt sein:

**Katalog der Notfallmaßnahmen**
: Aufzeichnen der entsprechenden Notfallmaßnahmen bei Feuer, Naturkatastrophen oder anderen Aktivitäten zum Schutz der Mitarbeiter und zur Schadensbegrenzung.

**Sicherungsprozeduren**
: Sicherstellen, dass die wichtigsten Datenverarbeitungsfunktionen nach der Unterbrechung ausgeführt werden können.

**Wiederherstellungsprozeduren**

Erleichtern einer schnellen Wiederherstellung des Datenverarbeitungssystems nach einem Notfall.

*Prüfliste für die im Notfall auszuführenden Maßnahmen*

1. Starten des Plans
   a. Geschäftsleitung benachrichtigen.
   b. Die für die Wiederherstellung nach einem Katastrophenfall zuständigen Mitarbeiter benachrichtigen und einsetzen.
   c. Ausmaß des Notfalls feststellen.
   d. Abhängig vom Ausmaß des Notfalls den korrekten Plan zur Wiederherstellung der Anwendungen auswählen (siehe „Abschnitt 7. Wiederherstellungsplan–Mobiler Standort" auf Seite 15).
   e. Den Fortschritt überwachen.
   f. Den Ausweichstandort informieren und einen Zeitplan festlegen.
   g. Alle weiteren betroffenen Mitarbeiter informieren—sowohl die Benutzer als auch die Mitarbeiter in der Datenverarbeitung.
   h. Lieferanten informieren—sowohl für Hardware als auch für Software.
   i. Benutzer über die Serviceunterbrechung unterrichten.
2. Prüfliste (Folgeliste)
   a. Liste der Teams und der Aufgaben jedes Teams erstellen.
   b. Erforderliches Kapital besorgen und, falls erforderlich, Transportmöglichkeiten zum/vom Ausweichstandort einrichten.
   c. Falls erforderlich, Unterkünfte einrichten.
   d. Verpflegungseinrichtungen nach Bedarf organisieren.
   e. Liste aller Mitarbeiter mit Telefonnummern erstellen.
   f. Plan für die Mitwirkung der Benutzer erstellen.
   g. Zustellung und Empfang von Post sicherstellen.
   h. Bürobedarf für den Notfall bereitstellen.
   i. Nach Bedarf Geräte mieten oder erwerben.
   j. Feststellen, welche Anwendungen ausgeführt werden müssen und in welcher Reihenfolge.
   k. Anzahl der erforderlichen Datenstationen feststellen.
   l. Feststellen, welche Offline-Geräte für jede Anwendung erforderlich sind.
   m. Prüfen, ob alle für die Anwendung erforderlichen Formulare vorhanden sind.
   n. Alle für den Ausweichstandort bestimmten Daten prüfen, bevor der Heimatstandort verlassen wird, und das Hardwareprofil am Heimatstandort lassen.
   o. Die Hauptlieferanten bestimmen, die bei den durch den Notfall entstandenen Problemen eventuell helfen können.
   p. Den Transport zusätzlich benötigter Ausrüstung zum Ausweichstandort planen.
   q. Streckenpläne/Stadtplan zum Ausweichstandort bereithalten.
   r. Prüfen, ob bei Bedarf zusätzliche Magnetbänder vorhanden sind.
   s. System- und betriebsbezogene Dokumentation sowie Kopie(n) der Wiederherstellungsprozeduren mitnehmen.
   t. Sicherstellen, dass alle betroffenen Mitarbeiter ihre Aufgaben kennen.
   u. Versicherungsgesellschaften benachrichtigen.

*Startprozeduren für die Wiederherstellung nach einem Notfall*

1. Den Wiederherstellungsservice _____ über den Notfall und die ausgewählten Wiederherstellungsprozeduren informieren.

**Anmerkung:** Die garantierte Durchführungszeit läuft ab dem Zeitpunkt, zu dem _____ über die ausgewählten Wiederherstellungsprozeduren informiert wird.

a. Telefonnummern für den Notfall

_____ oder _____

Diese Telefonnummern sind Montag bis Freitag von _____ Uhr bis _____ Uhr erreichbar.

2. Telefonnummer für den Notfall: _____

   Diese Telefonnummer ist für Notfälle außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen bestimmt. Diese Nummer bitte nur benutzen, um einen eingetretenen Notfall mitzuteilen.

3. _____ eine Adresse zur Anlieferung von Geräten (falls erforderlich), eine Kontaktadresse und eine alternative Kontaktadresse zur Koordinierung von Services und Telefonnummern, die 24 Stunden am Tag erreichbar sind, mitteilen.
4. Die Stromversorgungs- und Telefonunternehmen unterrichten und die erforderlichen Serviceverbindungen planen.
5. _____ sofort informieren, wenn zugehörige Pläne geändert werden.

## Abschnitt 7. Wiederherstellungsplan–Mobiler Standort

1. _____ über die Art des Notfalls unterrichten und darüber informieren, dass der Wiederherstellungsplan für einen mobilen Standort benutzt werden soll.
2. Innerhalb von 48 Stunden die telefonische Benachrichtigung von _____ schriftlich bestätigen.
3. Sicherstellen, dass alle erforderlichen Sicherungsdatenträger zum Laden des Ausweichsystems zur Verfügung stehen.
4. Die Ausweichgeräte schriftlich bestellen.
5. _____ über die bevorstehende Ankunft des Transporters mit dem mobilen Rechenzentrum und über den Abstellort des Transporters informieren (auf der _____ Seite von _____). (Siehe Plan für den mobilen Standort in diesem Abschnitt.)
6. Abhängig von den Fernsprecherfordernissen das Telefonunternehmen (_____) über mögliche Änderungen der Notleitungen informieren.
7. Mit dem Einrichten der Strom- und Fernsprechverbindungen bei _____ beginnen.
   a. Strom- und Fernsprechleitungen sollten für den Anschluss vorbereitet sein, wenn der Transporter mit dem mobilen Rechenzentrum eintrifft.
   b. An der Stelle, an der die Telefonleitungen in das Gebäude führen (_____), die aktuelle Verbindung mit den Verwaltungs-Controllern (_____) unterbrechen. Diese Leitungen werden zu Leitungen umgeleitet, die zum mobilen Rechenzentrum führen. Sie werden mit Modems im mobilen Rechenzentrum verbunden.

      Die Leitungen, die zur Zeit von _____ nach _____ führen, werden dann an das mobile Rechenzentrum über Modems angeschlossen.
   c. Möglicherweise erfordert dies, dass _____ Leitungen bei _____ in einen geschützteren Bereich für den Fall eines Notfalls umleitet.
8. Nach Ankunft des Transporters die Stromversorgung herstellen und die notwendigen Prüfungen durchführen.
9. Verbindung zu den Übertragungsleitungen herstellen und die notwendigen Prüfungen durchführen.
10. Laden des Systems mit Hilfe der Sicherungsdatenträger beginnen (siehe „Abschnitt 9. Das gesamte System zurückspeichern” auf Seite 17.)
11. Den normalen Betrieb so bald wie möglich wieder aufnehmen:
    a. Tägliche Jobs
    b. Tägliche Sicherungen
    c. Wöchentliche Sicherungen

12. Einen Zeitplan für die Sicherung des Systems erstellen, um das Zurückspeichern in das Basissystem am Ausgangsstandort vorzubereiten, nachdem es wieder verfügbar ist. (Die normalen Systemsicherungsprozeduren verwenden.)
13. Das mobile Rechenzentrum sichern und die Schlüssel nach Bedarf verteilen.
14. Ein Wartungsprotokoll für die Geräte des mobilen Rechenzentrums führen.

***Plan für den Aufbau des mobilen Rechenzentrums***

Den Plan für den Aufbau des mobilen Rechenzentrums hier beifügen.

***Plan für einen Notfall im Kommunikationsbereich***

Hier den Plan für einen Notfall im Kommunikationsbereich einschließlich der Schaltbilder beifügen.

***Kundennetzschaltplan***

Hier den Kundennetzschaltplan beifügen.

## Abschnitt 8. Wiederherstellungsplan–Ersatzstandort

Der Wiederherstellungsservice für Notfälle stellt einen alternativen Standort (Ersatzstandort) zur Verfügung. An diesem Standort ist ein Ausweichsystem vorhanden, das vorübergehend benutzt werden kann, während der Ausgangsstandort wiederhergestellt wird.

1. _____ über die Art des Notfalls unterrichten und mitteilen, dass der Wunsch besteht, einen Ersatzstandort einzurichten.
2. Anfordern, dass Modems für die Kommunikation per Luftfracht an _____ gesendet werden. (Informationen zu den DFV-Verbindungen für den Ersatzstandort bei _____ erfragen.)
3. Innerhalb von 48 Stunden die telefonische Benachrichtigung von _____ schriftlich bestätigen.
4. Mit den erforderlichen Reisevorbereitungen für das Einsatzteam beginnen.
5. Sicherstellen, dass alle erforderlichen Bänder zur Verfügung stehen und transportfertig verpackt sind, damit sie für die Wiederherstellung auf dem Ausweichsystem verwendet werden können.
6. Das Ausweichsystem schriftlich bestellen.
7. Anhand der Prüfliste vor der Abfahrt an den Ersatzstandort prüfen, ob das gesamte erforderliche Material dabei ist.
8. Prüfen, ob dem Wiederherstellungsteam die erforderlichen Informationen vorliegen, um mit dem Wiederherstellen des ursprünglichen Standorts zu beginnen. (Siehe „Abschnitt 12. Wiederherstellen des zerstörten Standorts" auf Seite 19).
9. Reisekosten decken (Vorschuss).
10. Nach Ankunft am Ersatzstandort Kontakt mit dem Heimatstandort aufnehmen, um die Übertragungsverbindung einzurichten.
11. Prüfen, ob das an den Ersatzstandort gebrachte Material vollständig ist.
12. Mit dem Laden des Systems von den Sicherungsbändern beginnen.
13. Den normalen Betrieb so bald wie möglich wieder aufnehmen:
    a. Tägliche Jobs
    b. Tägliche Sicherungen
    c. Wöchentliche Sicherungen
14. Einen Zeitplan für die Sicherung des Ersatzstandortsystems ausarbeiten, um in das System am Ausgangsstandort zurückspeichern zu können.

***Systemkonfiguration für den Ersatzstandort***

Hier die Systemkonfiguration für den Ersatzstandort beifügen.

## Abschnitt 9. Das gesamte System zurückspeichern

Um das System so wiederherzustellen, wie es vor dem Notfall benutzt wurde, verwenden Sie die im Handbuch *Sicherung und Wiederherstellung, IBM Form SC42-2053-08*, beschriebenen Prozeduren für die Wiederherstellung nach einem vollständigen Systemausfall.

*Erste Schritte:* Holen Sie folgende Bänder, Geräte und Unterlagen aus dem Sicherheitsraum vor Ort oder aus dem Aufbewahrungsort außerhalb des Unternehmens:

- Wenn Sie von der alternativen Installationseinheit installieren, sind sowohl die Banddatenträger als auch die CD-ROM mit dem lizenzierten internen Code erforderlich.
- Alle Bänder der letzten vollständigen Sicherung
- Die Bänder, auf die zuletzt die Sicherheitsdaten gesichert wurden (SAVSECDTA oder SAVSYS)
- Die neuesten Bänder mit der gesicherten Konfiguration, falls erforderlich
- Alle Bänder mit Journalen und Journalempfängern, die nach der letzten täglichen Sicherung gesichert wurden
- Alle Bänder der letzten täglichen Sicherung
- PTF-Liste, die mit den Sicherungsbändern der letzten vollständigen Sicherung und/oder der letzten wöchentlichen Sicherung aufbewahrt wird
- Liste der Bänder der letzten vollständigen Sicherung
- Liste der Bänder der letzten wöchentlichen Sicherung
- Liste der Bänder der täglichen Sicherungen
- Systemprotokoll der letzten vollständigen Sicherung
- Systemprotokoll der letzten wöchentlichen Sicherung
- Systemprotokoll der täglichen Sicherungen
- Das Handbuch *i5/OS und zugehörige Software installieren, löschen oder Upgrade durchführen*
- Das Handbuch *Sicherung und Wiederherstellung*
- Telefonverzeichnis
- Modemhandbuch
- Toolkit

## Abschnitt 10. Wiederherstellungsprozess

Das Management-Team muss das Ausmaß des Schadens beurteilen und mit dem Aufbau eines neuen Rechenzentrums beginnen.

Wenn der ursprüngliche Standort wiederhergestellt oder ersetzt werden muss, sollten unter anderem folgende Faktoren berücksichtigt werden:

- Wie hoch ist die geplante Verfügbarkeit aller benötigten Computereinheiten?
- Ist es günstiger, die Computersysteme durch neue Geräte zu ersetzen?
- Wie lange werden die Reparaturen oder der Aufbau des Rechenzentrums voraussichtlich dauern?
- Gibt es einen Alternativstandort, der schneller zu Datenverarbeitungszwecken aufgerüstet werden kann?

Wenn die Entscheidung getroffen wurde, das Rechenzentrum wiederaufzubauen, fahren Sie mit „Abschnitt 12. Wiederherstellen des zerstörten Standorts" auf Seite 19 fort.

## Abschnitt 11. Plan zur Wiederherstellung nach einem Katastrophenfall testen

Für eine erfolgreiche Planung für den Notfall ist es wichtig, den Plan regelmäßig zu testen und zu bewerten. Die Datenverarbeitung ist naturgemäß einem ständigen Wandel unterworfen, der Veränderungen bei

der Ausrüstung, bei den Programmen und bei der Dokumentation mit sich bringt. Daher ist es besonders wichtig, den Plan als ein sich änderndes Dokument zu betrachten. Gehen Sie beim Test anhand der Prüflisten vor und entscheiden Sie, welche Bereiche getestet werden sollten.

*Tabelle 8. Ausführen eines Wiederherstellungstests*

| Bereich | Ja | Nein | Zutreffend | Nicht zutreffend | Kommentare |
|---|---|---|---|---|---|
| Zweck des Tests bestimmen. Welche Teile des Plans werden beurteilt? | | | | | |
| Testziele beschreiben. Wie wird das Erreichen der Ziele gemessen? | | | | | |
| Den Management-Verantwortlichen den Test und seine Ziele erklären. Einverständnis einholen und Unterstützung zusichern lassen. | | | | | |
| Den Test und die ungefähre Dauer der Ausführung durch die Management-Verantwortlichen bekannt geben lassen. | | | | | |
| Testergebnisse am Ende der Testperiode sammeln. | | | | | |
| Ergebnisse auswerten. War die Wiederherstellung erfolgreich? Gründe? | | | | | |
| Folgerungen aus den Testergebnissen ableiten. Bedeutet die erfolgreiche Wiederherstellung in einem einfachen Fall auch, dass alle kritischen Jobs in einer akzeptablen Zeit erfolgreich wiederhergestellt werden können? | | | | | |
| Empfehlungen für Verbesserungen ausarbeiten. Antworten und Reaktionen bis zu einem bestimmten Zeitpunkt anfordern. | | | | | |
| Andere Bereiche über die Ergebnisse informieren. Dabei auch Benutzer und Sicherheitsprüfer informieren. | | | | | |
| Den Plan zur Wiederherstellung bei Notfällen bei Bedarf ändern. | | | | | |

*Tabelle 9. Zu testende Bereiche*

| Bereich | Ja | Nein | Zutreffend | Nicht zutreffend | Kommentare |
|---|---|---|---|---|---|
| Wiederherstellung der einzelnen Anwendungssysteme mit Dateien und Dokumentation, die an einem anderen Standort außerhalb des Unternehmens aufbewahrt werden. | | | | | |
| Erneutes Laden der Systembänder und Durchführen eines IPL mit Dateien und Dokumentation, die an einem Standort außerhalb des Unternehmens aufbewahrt werden. | | | | | |
| Möglichkeit der Verarbeitung auf einem anderen Computer. | | | | | |
| Kann das Management die Priorität von Systemen bestimmen, falls nur eingeschränkte Verarbeitungsmöglichkeiten vorliegen? | | | | | |

*Tabelle 9. Zu testende Bereiche (Forts.)*

| Bereich | Ja | Nein | Zutreffend | Nicht zutreffend | Kommentare |
|---|---|---|---|---|---|
| Kann die Wiederherstellung und Verarbeitung auch ohne die eigentlich dafür vorgesehenen Mitarbeiter erfolgreich durchgeführt werden? | | | | | |
| Enthält der Plan klare Aussagen über Zuständigkeiten und Befehlswege. | | | | | |
| Effizienz der Sicherheitsmaßnahmen und Prozeduren zur Sicherheitsumgehung während der Wiederherstellung. | | | | | |
| Ist eine Notfallevakuierung möglich und werden grundlegende Erste-Hilfe-Erfordernisse erfüllt? | | | | | |
| Kommen Benutzer von Echtzeitsystemen mit dem temporären Fehlen von Onlineinformationen zurecht? | | | | | |
| Können Benutzer tägliche Operationen ohne Anwendungen oder Jobs, die als nicht kritisch eingestuft werden, fortsetzen? | | | | | |
| Kann rasch Kontakt zu wichtigen Personen oder deren Stellvertretern aufgenommen werden? | | | | | |
| Kann die Dateneingabe bei kritischen Systemen über alternative Standorte und andere Eingabemedien erfolgen? | | | | | |
| Sind Peripheriegeräte wie Drucker und Scanner verfügbar und einsatzbereit? | | | | | |
| Ist Zusatzausrüstung verfügbar (beispielsweise Klimaanlage und Luftfeuchtigkeitsregler)? | | | | | |
| Verfügbarkeit von Hilfeleistungen bei Zubehör, Transport und Leitungen. | | | | | |
| Verteilung der am Wiederherstellungsstandort erstellten Ausgabe. | | | | | |
| Verfügbarkeit von wichtigen Formularen und Papier. | | | | | |
| Möglichkeit, den Plan an weniger große Notfälle anzupassen. | | | | | |

## Abschnitt 12. Wiederherstellen des zerstörten Standorts

- Grundriss des Rechenzentrums.
- Die aktuellen Hardwareerfordernisse und mögliche Alternativen feststellen. (Siehe „Abschnitt 4. Hardwareprofil" auf Seite 12.)
- Grundfläche des Rechenzentrums, Elektrizitätsbedarf und Sicherheitsanforderungen.
  - Grundfläche (m²) _____
  - Elektrizitätsbedarf _____
  - Sicherheitsanforderungen: Abschließbare Räume, vorzugsweise Kombinationsschloss an einer Tür.
  - Raumaufteilung
  - Detektoren für überhöhte Temperatur, Wasser, Rauch, Feuer und Erschütterungen
  - Doppelboden

*Lieferanten*

*Grundriss*

Hier eine Kopie des möglichen Grundrisses beifügen.

## Abschnitt 13. Aufzeichnung von Planänderungen

Halten Sie den Plan immer auf dem neuesten Stand. Fertigen Sie Unterlagen über Änderungen an der Konfiguration, an Anwendungen, Sicherungszeiten und -prozeduren an. Sie können beispielsweise eine Liste der aktuellen lokalen Hardware durch Eingabe des folgenden Befehls drucken:

```
DSPHDWRSC OUTPUT(*PRINT)
```

**Zugehörige Informationen**

DSPHDWRSC

# Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris La Defense Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_. Alle Rechte vorbehalten.

## Marken

Folgende Namen sind in gewissen Ländern (oder Regionen) Marken der International Business Machines Corporation:

- eServer
- IBM
- IBM(logo)
- iSeries
- i5/OS

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

## Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

**Persönliche Nutzung:** Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

**Kommerzielle Nutzung:** Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf ″as-is″-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.