



System i

Systemverwaltung

Planung einer Sicherungs-  
und Wiederherstellungsstrategie

*Version 6 Release 1*







System i

Systemverwaltung

Planung einer Sicherungs-  
und Wiederherstellungsstrategie

*Version 6 Release 1*

**Hinweis**

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

Diese Ausgabe bezieht sich auf Version 6, Release 1, Modifikation 0 von IBM i5/OS (Produktnummer 5761-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 System i Systems management, Planning a backup and recovery strategy, Version 6 Release 1*,  
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2000, 2008  
© Copyright IBM Deutschland GmbH 2008

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:  
SW TSC Germany  
Kst. 2877  
Februar 2008

---

# Inhaltsverzeichnis

## Planung einer Sicherungs- und Wiederherstellungsstrategie . . . . . 1

PDF-Datei für Planung einer Sicherungs- und Wiederherstellungsstrategie . . . . .	1
Zeitraumen für Sicherung und Wiederherstellung . . . . .	2
Zu sichernde Daten und Häufigkeit der Sicherungen festlegen. . . . .	3
Sicherungsfenster bestimmen . . . . .	4
Einfache Sicherungsstrategie . . . . .	5
Mittlere Sicherungsstrategie . . . . .	5
Geänderte Objekte sichern. . . . .	6
Objekte aufzeichnen und Journalempfänger sichern . . . . .	6

Komplexe Sicherungsstrategie . . . . .	7
Verfügbarkeitsoptionen auswählen . . . . .	8
Strategie testen . . . . .	9
Wiederherstellung nach einem Katastrophenfall planen . . . . .	9
Plan zur Wiederherstellung nach einem Katastrophenfall . . . . .	9

## Anhang. Bemerkungen. . . . . 21

Informationen zu Programmierschnittstellen . . . . .	22
Marken. . . . .	23
Bedingungen . . . . .	23



---

# Planung einer Sicherungs- und Wiederherstellungsstrategie

Wenn Daten auf Ihrem System verloren gehen, benötigen Sie die Sicherungskopien dieser Daten. Diese Themensammlung enthält Informationen zum Planen einer Strategie und zu den Auswahlmöglichkeiten, die Sie beim Konfigurieren Ihres Systems hinsichtlich der Sicherung, Wiederherstellung und Verfügbarkeit treffen müssen.

Die IBM System i-Produkte sind sehr zuverlässig. 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 Computerproblemen 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?

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 sich mit dem Zeitrahmen für die Sicherung und Wiederherstellung beschäftigt haben, können Sie mit dem Planen Ihrer Strategie beginnen, indem Sie die folgenden Schritte ausführen:

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

## **Zugehörige Konzepte**

Sicherung des Systems

Roadmap zur Verfügbarkeit

## **Zugehörige Informationen**

Häufig gestellte Fragen zur Sicherung und Wiederherstellung

Sicherung und Wiederherstellung

---

## PDF-Datei für Planung einer Sicherungs- und Wiederherstellungsstrategie


Sie können eine PDF-Datei mit diesen Informationen anzeigen und drucken. Zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments wählen Sie Planung einer Sicherungs- und Wiederherstellungsstrategie aus.

### **PDF-Dateien sichern**

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

1. Klicken Sie mit der rechten Maustaste den PDF-Link in Ihrem Browser an.
2. Klicken Sie auf die Option, mit der die PDF lokal gespeichert wird.
3. Navigieren Sie zu dem Verzeichnis, in dem die PDF gespeichert werden soll.
4. Klicken Sie auf **Speichern**.

## Adobe Reader herunterladen

Adobe 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](http://www.adobe.com/products/acrobat/readstep.html))  herunterladen.

---

## Zeitrahmen für Sicherung und Wiederherstellung

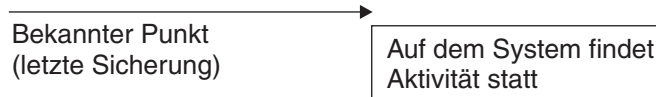
Der Zeitrahmen für die Sicherung und Wiederherstellung beginnt, wenn Sie die Informationen sichern, und endet, wenn Ihr System nach einem Ausfall vollständig wiederhergestellt wurde.

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

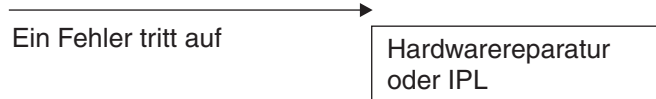
- Ob Sie jeden Schritt im Diagramm erfolgreich ausführen können.
- Wie lange Sie für die Ausführung jedes Schritts benötigen.

Verwenden Sie den folgenden Zeitrahmen, um spezielle Beispiele zu erstellen. Was wäre, wenn der bekannte Punkt (1) ein Sonntagabend und der Fehlerpunkt (2) ein Donnerstagnachmittag 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?

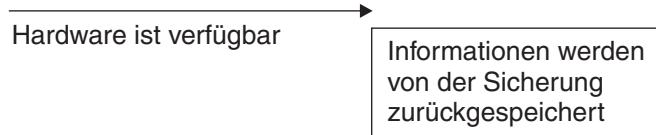
### Punkt 1



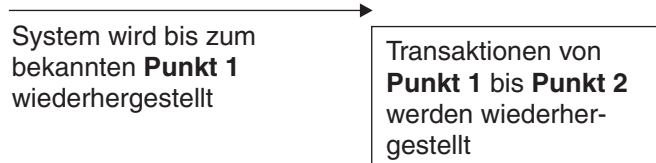
### Punkt 2



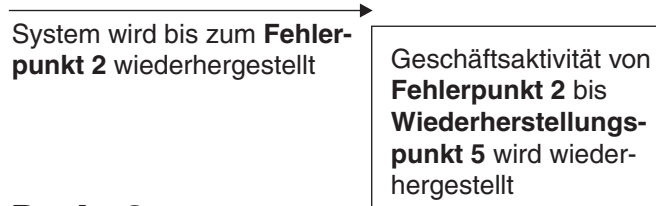
### Punkt 3



### Punkt 4



### Punkt 5



### Punkt 6



RZAJ1001-0

Es folgt die 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 einleitendes Programmladen (IPL) 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“

Teile des Systems, die häufigen Änderungen unterliegen, sollten Sie täglich sichern. Alle anderen Teile sollten wöchentlich gesichert werden.

---

## Zu sichernde Daten und Häufigkeit der Sicherungen festlegen

Teile des Systems, die häufigen Änderungen unterliegen, sollten Sie täglich sichern. Alle anderen Teile sollten wöchentlich gesichert werden.

Wenn Sie nicht regelmäßig alle Daten sichern, können Sie bei einem Standortverlust oder bei bestimmten Arten von Plattenfehlern keine Wiederherstellung durchführen. Wenn Sie die geeigneten Teile Ihres Systems sichern, können Sie bis zu Punkt 4, der beim Zeitrahmen für die Sicherung und Wiederherstellung gezeigt wird, wiederherstellen (letzte Sicherung).

### Teile des Systems, die häufigen Änderungen unterliegen

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

*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 <sup>1</sup>
Konfigurationsobjekte in QSYS	Nein	Regelmäßig, wenn Einheitenbeschreibungen hinzugefügt oder geändert werden oder wenn Sie die Funktion Hardware Service Manager verwenden, um die Konfigurationsdaten zu aktualisieren <sup>1</sup>
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

<sup>1</sup> Diese Objekte werden unter Umständen auch geändert, wenn Sie die Lizenzprogramme 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 (QHLPYSYS, QUSRTOOL)	Ja	PTFs oder ein neues Release des Betriebssystems
Lizenzprogrammbibliotheken (QRPG, QCBL, Qxxxx)	Ja	Aktualisierungen an den Lizenzprogrammen
Lizenzprogrammordner (Qxxxxxxx)	Ja	Aktualisierungen an den Lizenzprogrammen
Lizenzprogrammverzeichnisse (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Ja	Aktualisierungen an den Lizenzprogrammen

### Zugehörige Konzepte

„Zeitrahen für Sicherung und Wiederherstellung“ auf Seite 2

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

### Zugehörige Verweise

„Einfache Sicherungsstrategie“ auf Seite 5

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 alle Verfügbarkeitsoptionen des Systems, einschließlich Cluster, einer ernsthaften Bewertung unterziehen.

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

## 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 Bedieneringriff (nicht überwacht) 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 muss allerdings ausreichend Datenträgerkapazität für das Online-Backup 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  
Teile des Systems, die häufigen Änderungen unterliegen, sollten Sie täglich sichern. Alle anderen Teile sollten wöchentlich gesichert werden.

## Mittlere Sicherungsstrategie

Sie haben ein mittleres Sicherungsfenster, d. h., Ihnen steht täglich ein Zeitblock von vier bis sechs Stunden 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.

Wenn Sie nachts umfangreiche Stapeljobs auf Ihrem System ausführen oder wenn sehr große Dateien vorhanden sind, 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 folgende Verfahren 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) erlaubt Ihnen, nur die Dokumente und Ordner zu sichern, die sich geändert haben. Analog können Sie mit dem Befehl SAV (Save - Sichern) die Objekte in Verzeichnissen sichern, die sich seit einem bestimmten Zeitpunkt geändert haben.

Darüber hinaus können Sie sich 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 <sup>1</sup>
Dienstagnacht	Gering	Menü SICHERN, Option 23
Mittwochnacht	Groß	Nur Änderungen sichern <sup>1</sup>
Donnerstagnacht	Groß	Nur Änderungen sichern <sup>1</sup>
Freitagnacht	Gering	Menü SICHERN, Option 21

<sup>1</sup> Verwenden Sie eine Kombination aus den Befehlen SAVCHGOBJ, SAVDLO und SAV.

## Objekte aufzeichnen und Journalempfänger sichern

Wenn Ihre Sicherungsoperationen für IFS-Objekte und -Datenbereiche (IFS - integriertes Dateisystem) zu lange dauern, können Sie die Objekte aufzeichnen und die Sicherungsoperationen effizienter gestalten.

Wenn Sie eine Teildatei mit 100 000 Sätzen haben und sich 1 Satz ändert, sichert der Befehl SAVCHGOBJ (Geänderte Objekte sichern) 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. 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

Tabelle 3. Beispiel für Sicherungsstrategie (Forts.)

Tag	Stapelauslastung	Sicherungsoperation
Mittwochnacht	Groß	Journalempfänger sichern
Donnerstagnacht	Groß	Journalempfänger sichern
Freitagnacht	Gering	Menü SICHERN, Option 21

#### Anmerkungen:

- 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 können den Befehl SAVLIB (Bibliothek sichern) oder den Befehl SAVOBJ (Objekt sichern) verwenden.
- Neue Objekte müssen gesichert werden, bevor Journaleinträge für ein Objekt angewendet 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 Journaling.

#### Zugehörige Konzepte

Journal management

#### Zugehörige Verweise

l Change Journal Receiver Exit Program

## 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 bestimmte kritische Dateien zu bestimmten Tageszeiten oder an bestimmten Wochentagen sichern. Außerdem ist es sinnvoll, BRMS (Backup, Recovery and Media Services) zu verwenden.

Bei einer komplexen Sicherungsstrategie ist es oft erforderlich, das System zu sichern, während es aktiv ist. Der Parameter SAVACT (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, stehen die Objekte zwecks weitere Verwendung zur Verfügung. Die Befehle für die Sicherung im aktiven Zustand können Sie zusammen mit Journaling und Commitsteuerung verwenden, um die Wiederherstellungsprozedur zu vereinfachen. Wenn Sie beim Parameter SAVACT die Werte \*LIB oder \*SYNCLIB verwenden, sollten Sie mit Journaling arbeiten, um die Wiederherstellung zu vereinfachen. Wenn Sie beim Parameter SAVACT den Wert \*SYSDFN angeben, müssen Sie auch mit Commitsteuerung arbeiten, wenn die zu sichernde Bibliothek zusammen-

gehörige 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, oder Sie können 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 BRMS oder eine Anwendung, mit der Sie Datenträgerdefinitionsobjekte erstellen können.

#### **Zugehörige Konzepte**

Backup, Recovery and Media Services (BRMS)

Verwendung der Sicherung im aktiven Zustand im Rahmen Ihrer Sicherungs- und Wiederherstellungsstrategie

Daten zum Verkleinern Ihres Sicherungsfensters auf mehreren Einheiten sichern

System sichern

Commitment control

Journal management

---

## **Verfügbarkeitsoptionen auswählen**

Verfügbarkeitsoptionen sind Ergänzungen für eine gute Sicherungsstrategie, kein Ersatz. 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.
- Die Art Ihrer 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.

#### **Zugehörige Konzepte**

Roadmap zur Verfügbarkeit

## 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 Journaling 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. Sie können eine Wiederherstellung zwar auf Ihrem eigenen System ausführen, dies ist jedoch sehr riskant. Wenn Sie nicht alle Daten erfolgreich sichern, gehen bei der versuchten Wiederherstellung möglicherweise Daten verloren.

Eine ganze Reihe von Organisationen bieten Tests für Wiederherstellungen als Dienstleistung an. Business

Continuity and Resiliency  ist eine solche Organisation, die Ihnen bei Wiederherstellungstests behilflich sein kann.

### Zugehörige Konzepte

„Zeitraumen für Sicherung und Wiederherstellung“ auf Seite 2

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

---

## Wiederherstellung nach einem Katastrophenfall planen

Diese Richtlinien enthalten die Informationen und Prozeduren, 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.

## Plan zur Wiederherstellung nach einem Katastrophenfall

Nachfolgend finden Sie eine Schablone, die Sie beim Erstellen eines Plans zur Wiederherstellung nach einem Katastrophenfall verwenden können.

## Abschnitt 1. Hauptziele dieses Plans

Die folgende Liste enthält die Hauptziele dieses Plans:

- 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



Tabelle 5. Anwendungsprofil (Forts.)

Anwendungsprofil				
Anwendungsname	Kritisch? Ja/Nein	Anlagevermögen? Ja/Nein	Hersteller	Kommentare
				<b>Legende für Kommentare:</b>
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
- Ersatzworkstations
- 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

Tabelle 6. Hardwareprofil (Forts.)

Hardwareprofil					
Hersteller	Beschreibung	Modell	Seriennummer	Gekauft oder geleast	Kosten
<b>Anmerkung:</b> Diese Liste sollte alle _____ Monate überprüft werden.					

Tabelle 7. Zubehör (Verschiedenes)

Zubehör (Verschiedenes)		
Beschreibung	Menge	Kommentare
<b>Anmerkung:</b> Diese Liste enthält Folgendes:		
<ul style="list-style-type: none"> <li>• Bänder</li> <li>• PC-Software</li> <li>• Akten oder Dokumentation</li> <li>• Bänder im Sicherheitsraum</li> <li>• Disketten</li> <li>• Emulationspakete</li> <li>• Programmiersprachensoftware</li> <li>• Druckerzubehör (wie Papier und Formulare)</li> </ul>		

## Abschnitt 5. Sicherungsprozeduren für Informationsservices

- i5/OSBetriebssystem
  - Täglich: Journalempfänger werden um \_\_\_\_\_ Uhr und um \_\_\_\_\_ Uhr geändert.
  - Täglich: Geänderte Objekte in den folgenden Bibliotheken und Verzeichnissen werden um \_\_\_\_\_ Uhr gesichert:
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
    - \_\_\_\_\_
  - Mit dieser Prozedur werden auch die Journale und Journalempfänger gesichert.
  - Am \_\_\_\_\_ (Tag) um \_\_\_\_\_ Uhr wird eine vollständige Sicherungsoperation für das System 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. Die Kopien der PC-Dateien sollten unmittelbar vor der vollständigen Sicherungsoperation für das System am \_\_\_\_\_ (Datum) um \_\_\_\_\_ Uhr auf das System hochgeladen werden. Das System wird mit der normalen System-

sicherungsprozedur gesichert. Auf diese Weise wird eine zuverlässigere Sicherung von PC-bezogenen Systemen erreicht, bei denen durch einen lokalen Notfall unter Umständen Daten wichtiger PC-Systeme gelöscht werden.

## **Abschnitt 6. Prozeduren zur Wiederherstellung nach einem Katastrophenfall**

Bei allen Plänen 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 einer Katastrophe.

### **Prüfliste für die nach einem Katastrophenfall auszuführenden Maßnahmen:**

1. Starten des Plans
  - a. Höheres Management 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 einen geeigneten Plan zur Wiederherstellung der Anwendungen auswählen (siehe „Abschnitt 7. Wiederherstellungsplan - Mobiler Standort“ auf Seite 14).
  - e. Den Fortschritt überwachen.
  - f. Die Ausweichstandorte informieren und die Zeitpläne 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 für Folgeaktionen:
  - a. Liste der Teams und der Aufgaben jedes Teams erstellen.
  - b. Erforderliches Kapital besorgen und Transportmöglichkeiten zum/vom Ausweichstandort einrichten.
  - c. Unterkünfte einrichten.
  - d. Verpflegungseinrichtungen organisieren.
  - e. Liste aller Mitarbeiter mit Telefonnummern erstellen.
  - f. Pläne 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. Strecken-/Stadtpläne zum Ausweichstandort bereithalten.
- r. Prüfen, ob 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 Katastrophenfall:**

1. Den Wiederherstellungsservice \_\_\_\_\_ über den Katastrophenfall 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 müssen.

### **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 Kernpunkte der telefonischen 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 Verwaltungscontrollern (\_\_\_\_\_) 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 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 16.)
- 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 System-sicherungsprozeduren 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.

**Stromversorgung:**

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**

Führen Sie die im Thema Systemverwaltung: Sicherung und Wiederherstellung beschriebenen Prozeduren für die Wiederherstellung nach einem vollständigen Systemausfall aus, um das System so wiederherzustellen, wie es vor dem Notfall benutzt wurde.

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 neuesten vollständigen Sicherungsoperation.
- Die neuesten Bänder, auf die die Sicherheitsdaten gesichert wurden (SAVSECDTA oder SAVSYS).
- Die neuesten Bänder mit der gesicherten Konfiguration.
- Alle Bänder mit Journalen und Journalempfängern, die nach der neuesten täglichen Sicherungsoperation gesichert wurden.
- Alle Bänder der neuesten täglichen Sicherungsoperation.
- Liste der vorläufigen Programmkorrekturen (PTFs), die mit den Sicherungsbändern der neuesten vollständigen Sicherung und/oder der neuesten wöchentlichen Sicherung aufbewahrt wird.
- Liste der Bänder der neuesten vollständigen Sicherungsoperation.
- Liste der Bänder der neuesten wöchentlichen Sicherungsoperation.
- Liste der Bänder der täglichen Sicherungen.
- Systemprotokoll der neuesten vollständigen Sicherungsoperation.
- Systemprotokoll der neuesten wöchentlichen Sicherungsoperation.
- Systemprotokoll der täglichen Sicherungsoperationen.
- Die Themensammlung i5/OS und zugehörige Software installieren, löschen oder Upgrade durchführen.
- Die Themensammlung Systemverwaltung: 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, müssen Sie die folgenden Faktoren berücksichtigen:

- 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?

Nachdem die Entscheidung getroffen wurde, das Rechenzentrum wiederaufzubauen, mit „Abschnitt 12. Wiederherstellen des zerstörten Standorts“ auf Seite 19 fortfahren.

## 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 Managementverantwortlichen den Test und seine Ziele erklären. Einverständnis einholen und Unterstützung zusichern lassen.					
Den Test und die ungefähre Dauer der Ausführung durch die Managementverantwortlichen bekannt geben lassen.					
Testergebnisse am Ende der Testperiode sammeln.					
Ergebnisse auswerten. Ist die Wiederherstellung erfolgreich? Gründe für den Erfolg/Misserfolg?					
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 nach einem Katastrophenfall 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 einleitenden Programmladens (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?					
Kann die Wiederherstellung und Verarbeitung auch ohne die eigentlich dafür vorgesehenen Mitarbeiter erfolgreich durchgeführt werden?					
Enthält der Plan klare Aussagen über Zuständigkeitsbereiche und Befehlswege.					
Effektivität der Sicherheitsmaßnahmen und Prozeduren zur Sicherheitsumgehung während der Wiederherstellung.					
Ist eine Notfalleвакуierung möglich und werden grundlegende Erste-Hilfe-Erfordernisse erfüllt?					
Können 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 11.)
- Grundfläche des Rechenzentrums, Elektrizitätsbedarf und Sicherheitsanforderungen.
  - Grundfläche (m<sup>2</sup>) \_\_\_\_\_.
  - Elektrizitätsbedarf \_\_\_\_\_.
  - Sicherheitsanforderungen: Abschließbare Räume, vorzugsweise Kombinationsschloss an einer Tür.
  - Raumhohes Ständerwerk.
  - Detektoren für überhöhte Temperatur, Wasser, Rauch, Feuer und Erschütterungen.
  - Hohlraumboden

### **Lieferanten:**

### **Grundriss:**

Hier eine Kopie des möglichen Grundrisses beifügen.

## **Abschnitt 13. Aufzeichnung von Planänderungen**

Bewahren Sie Ihren aktuellen Plan auf. 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**

Display Hardware Resources (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 Director of Licensing  
IBM Europe, Middle East & Africa  
Tour Descartes  
2, avenue Gambetta  
92066 Paris La Defense  
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 Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials  
| erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungs-  
| bedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalen-  
| ten 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 Quellsprache 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.

---

## | Informationen zu Programmierschnittstellen

In der vorliegenden Veröffentlichung Planung einer Sicherungs- und Wiederherstellungsstrategie werden vorgesehene Programmierschnittstellen dokumentiert, mit deren Hilfe Kunden Programme zum Abrufen von IBM i5/OS-Services schreiben können.

---

## Marken

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

IBM  
IBM(logo)  
System i  
i5/OS

- | Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind in gewissen Ländern eingetragene Marken oder Marken von Adobe Systems Incorporated.

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 Veröffentlichungen. 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.





**IBM**