# Datensicherungskonzept Westfälische Hochschule

-ZIM-

Rev. 1.00
Stand: 04.04.2014

**Revisionsstände**

| Revisionsstand | Kommentar |
|---|---|
| 1.00 | Erste Version |

# 1 Einleitung

Das Datensicherungskonzept dient zur Dokumentation der in der Hochschule geltenden Regelungen und ergriffenen Maßnahmen zur Datensicherung. Damit sollen die vom ZIM durchgeführten Sicherungs-/Wiederherstellungsmethoden transparent für alle Nutzer dargestellt werden.

Alle von dem ZIM betriebenen Server sind mit redundanten Festplatten ausgestattet. Sei es mit lokalen Platten in einem RAID 1 oder RAID5 System oder in einem Storage Area Network, bei dem die Daten in getrennten Brandabschnitten gespiegelt vorliegen.
Trotzdem kann es Situationen geben, bei denen durch äußere Einwirkungen oder durch menschliche Fehler die Daten auf den Festplatten nicht mehr lesbar sind. Weiterhin fällt das Fehlen einer gelöschten Datei nicht sofort auf. Somit müssen aktuell gelöschte Dateien über einen gewissen Zeitraum wiederherstellbar sein.

## 1.1 Spezifikation der zu sichernden Daten

Prinzipiell werden alle Daten von ZIM betriebenen Servern gesichert. Darunter fallen explizit:

- Anwendungs- und Betriebssoftware
- Systemdaten
- Anwendungsdaten / Benutzerdaten
- Datenbanken (je nach Datenbanksoftware werden geeignete Sicherungsarten gewählt)
- Software

In der Regel ist das ZIM nicht Datenverantwortlicher und besitzt somit keine Kenntnisse über die Wichtigkeit oder die Verfügbarkeitsanforderungen von Applikationen und Daten. Deshalb werden per se alle Daten gleich behandelt, wenn nicht Sondervereinbarungen existieren.

## 1.2 Datensicherungsart

Für die Backup Strategie wurde das bewährte Konzept „Disk-to-Disk-to-Tape“ (D2D2T) umgesetzt. Täglich werden alle virtuellen Server als Snapshot auf ein Festplatten-Array des Backupservers abgelegt. Samstags als Full Backup, Sonntags bis Freitags als Incremental Backup. Freitags werden alle Sicherungen der vorangegangenen 7 Tage auf Tape gesichert.

Für ein schnelles Desaster Recovery ist die Kapazität des Disk-Arrays so ausgelegt, dass zu jedem Zeitpunkt auf die Sicherung der vorangegangenen 7 Tage zugegriffen werden kann. Ältere Sicherungen (8 Tage – 3 Monate) müssen vom Tape restauriert werden, was entsprechend länger dauert.

Aktuelle Dateien befinden sich ständig in der Sicherung. Gelöschte Dateien können bis maximal 3 Monate nach der Löschung noch wiederhergestellt werden.

## 1.3 Infrastruktur

Für die Datensicherung wird folgende Infrastruktur genutzt.

| | |
|---|---|
| Backupserver: | HP DL380 |
| Staging Disk | 7 Terabyte |
| Tape Library: | HP MSL 4048 |
| Bandlaufwerke: | 2x HP Ultrium SCSI LTO 5 |
| Bänder | LTO 5 |

Die Tape Library beinhaltet insgesamt 48x LTO5 Bänder. Ausgestattet ist diese mit 2 Bandlaufwerken, die unabhängig voneinander betrieben werden können.
Es werden die von dem Hersteller des Datensicherungssystems spezifizierten Medien genutzt. Reinigungsintervalle der Bandlaufwerke werden gemäß Herstellerhandbuch oder nach Anzeige des Datensicherungsgeräts vorgenommen.

Als Datensicherungssoftware wird „Veeam Backup&Restore Enterprise“ eingesetzt.

# 2 Vorgehensweise

## 2.1 Zeitfenster für ein Backup

Die Dauer einer Sicherung hängt im Wesentlichen von der Anzahl und der Größe der zu sichernden Dateien ab. Einen genauen Zeitpunkt für den Sicherungsbeginn eines Servers kann deshalb nicht genannt werden. Der Beginn der Sicherungen findet jeden Tag um 0:00 Uhr statt. Die Backupinfrastruktur ist so ausgelegt, dass am Samstag (Full backup) spätestens um 10:00 Uhr und Sonntags-Freitags (Incremental Backup) spätestens um 02:00 Uhr alle Daten gesichert wurden.

## 2.2 Rekonstruktion von Daten

Ohne Datensicherung besteht keine Möglichkeit, zerstörte oder gelöschte Datenbestände wieder zu rekonstruieren. Das ZIM kann Daten nur für die von ihr betreuten Server zurückspielen.

Vom Anwender oder einer Applikation gelöschte Dateien werden nach 3 Monaten auch von den Sicherungsbändern gelöscht und sind damit nicht wiederherstellbar.

Prinzipiell werden alle Daten gesichert. Jedoch entstehen Lücken zwischen der letzten Datensicherung und dem aktuellen Zeitpunkt. Werden neue Daten in diesem Zeitraum erzeugt und auch wieder gelöscht, befinden sie sich noch nicht auf einem Sicherungsmedium. Die Daten sind in diesem Fall unwiederbringlich verloren. Beim Standardsicherungsverfahren kann der Zeitraum dieser Lücke maximal 24 Stunden betragen.

Besteht für eine Anwendung ein Bedarf an einer Verkleinerung dieser Lücke, so muss speziell für die Anwendung ein Sonderverfahren zur Datensicherung mit den Datenverantwortlichen entwickelt werden.

## 2.3 Rekonstruktionszeiten

Die Wiederherstellungsdauer von Daten hängt im Wesentlichen von der Anzahl und der Größe der zu rekonstruierenden Dateien ab. Befinden sich die Daten auf Tape, so verlängert sich die Zeit entsprechend.

Müssen im Desaster Fall mehrere Server zurückgespielt werden, so spielt das ZIM Server, welche unbedingt benötigte Basisfunktionalitäten wie z.B. DNS, DHCP oder Verzeichnisdienste erbringen, mit hoher Priorität zurück.

### 2.3.1 Verantwortlicher für die Datenwiederherstellung

Eine Datenwiederherstellung kann aufgrund nicht aktueller Daten für die betroffenen Nutzer eine große Auswirkung haben. Das ZIM spielt Daten nur in Absprache mit den Verantwortlichen der betroffenen Stelle zurück.
Nur die zuständigen Backup-Administratoren haben Zugriff auf die Backup-Daten.

## 2.4 Datensicherheit

Die Backup-Infrastruktur befindet sich innerhalb eines eigenen Brandabschnittes des Rechenzentrums. Die auszulagernden Magnetbänder kommen in einen speziellen Datensafe (magnetfeld-/staubgeschützte und klimagerechte Aufbewahrung), der sich wiederum in einem eigenen Brandabschnitt befindet. Zugriff haben nur die Mitarbeiter des RZ, zu deren Aufgaben die Datensicherung gehört.

# 3 Allgemeine Regelungen

## 3.1 Sicherung von Dateien der Benutzer

Das ZIM stellt allen Mitarbeitern Speicherplatz auf Servern für dienstliche Daten zur Verfügung, welcher in Form von Netzlaufwerken erreichbar ist. Alle Mitarbeiter/Innen müssen sämtliche dienstliche Daten auf den bekannten Netzlaufwerken ablegen, da nur die Inhalte dieser Laufwerke auch bei der Datensicherung mit berücksichtigt werden. Den Benutzern, welche sich an der Windows-Domäne „ZA“ anmelden, werden standardmäßig die Netzlaufwerke T:, Z: und U: zugeordnet. Diese Netzlaufwerke werden in mit dem normalen hier beschriebenen Verfahren gesichert.
Nicht Windows-User können sich die Netzlaufwerke ebenfalls entsprechend zuordnen. Auch hierbei gilt, dass alle auf dem zentralen Server (aktuell za-fs1-ge.za.w-hs.de) abgelegten Daten der normalen Sicherung unterworfen sind.

Daten, die hingegen auf dem lokalen Computer wie z.B. dem Laufwerk C: abgelegt werden, können bei der Datensicherung nicht berücksichtigt werden. Bei Datenverlust oder –Zerstörung können diese nicht wieder hergestellt werden.

## 3.2 Kontrollen der Datensicherung

Anhand von Protokollen der Sicherungssoftware wird täglich der korrekte Ablauf der Sicherungsjobs geprüft.

Bei fehlerhaften oder abgebrochenen Datensicherungen, besteht die Gefahr, dass betroffene Daten nicht zurückgesichert werden können. Wird bei der Kontrolle der Datensicherungen eine fehlerhafte Sicherung festgestellt, wird das Problem behoben und die entsprechende Sicherung noch einmal manuell angestoßen, soweit der reguläre Betrieb nicht durch diese Maßnahme gestört wird. Falls der Betrieb gestört wird, erfolgt die nächste Sicherung erst wieder nach dem normalen Schema.

Zusätzlich wird regelmäßig geprüft, ob mit den vorhandenen Sicherungskopien der Daten eine Rekonstruktion durchgeführt werden kann. Dieses wird alle vier Wochen, mit zufällig ausgesuchten Daten, durchgeführt.

Alle zwölf Wochen wird zufällig ein Server ausgewählt, welcher unter Laborbedingungen komplett aus dem Backup zurückgesichert und auf Lauffähigkeit hin überprüft wird.

## 3.3 Kenntnisnahmen

Die Inhalte des Datensicherungskonzeptes werden an geeigneter Stelle veröffentlicht. und ständig den aktuellen technologischen und organisatorischen Gegebenheiten angepasst. Aktuelle Informationen sind unter http://www.w-hs.de/backup zu finden.