



Parasol Island

Datensicherungs- und Archivierungsplan

Dateiname:	03_07_PSL_ISMS_Backup_und_Archiv_v01.00_cW
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	24.10.2017 Cedric Wolffs
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	24.10.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	20.09.2017	Justus Heinser	Anpassungen
00.03	17.10.2017	Cedric Wolffs	Anpassung Spezifikationen und Datensicherungsart Umbenennung 6. RAIDs zu 6. pslsrv10 Anpassung Infrastruktur
00.04	24.10.2017	Cedric Wolffs	Anpassung Datensicherungsart Auflistung der zu sichernden Verzeichnisse
01.00	24.10.2017	Cedric Wolffs	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Zielsetzung	3
2. Spezifikation der zu sichernden Daten	3
3. Datensicherungsart	3
4. Inkrementell	4
5. Archivierung	4
6. pslsrv10 und mobile Raids	4
7. Infrastruktur	4
8. Zeitfenster für ein Backup	5
9. Rekonstruktion von Daten	5
10. Rekonstruktionszeiten	5
11. Datensicherheit	5
12. Kontrollen der Datensicherungen	6
13. Sicherung von Dateien der Benutzer	6



Parasol Island

1. Zielsetzung

Der Datensicherungsplan soll eine exakte Arbeitsanweisung für die Ausführung des Datensicherungskonzeptes und somit die konkrete Umsetzung Richtlinien.

Der Plan soll Definieren welche Daten wie oft auf welche Art gesichert werden unter Berücksichtigung der Sicherheitsziele.

Die vorherige Klassifizierung der Daten ist zu berücksichtigen.

2. Spezifikation der zu sichernden Daten

Prinzipiell werden folgende Anwendungsdaten aus Verzeichnissen im Netzwerk gesichert:

- \\pslsrv10\Pipeline
- \\pslsrv10\Resources
- \\pslsrv10\Projects
- \\pslsrv25\Shares
- \\pslsrv10\Media

3. Datensicherungsart

Für die Server und Verzeichnisse gelten folgende Regelungen.

\\pslsrv10* \\pslsrv25\Shares	Inkrementell	Vollbackup	Archivierung
Häufigkeit	jeden Tag	halbjährlich	Nach Projekt Abschluss
Ausführung	1-Fach	1-Fach	2-Fach
Verschlüsselung	Ja (AES 256Bit)	Ja (AES 256Bit)	Ja (AES 256Bit)
Lagerung	Intern	Intern	Intern + Extern
Methode	Disk to Tape	Disk to Tape	Disk to Tape



Parasol Island

4. Inkrementell

Jeden Tag erfolgt ein verschlüsseltes inkrementelles Backup der Anwendungsdaten. Die Bandlaufwerke und Bänder befinden sich unter Verschluss in einem anderen Brandabschnitt.

Um den Rhythmus von inkrementellen Sicherungen zu erhöhen sind weitere Maßnahmen erforderlich:

- Verlegung des Datensicherungs Hard/Software Systems in einen anderen Brandabschnitt.
- Verlegung des Datensicherungsbestandes in einen anderen Brandabschnitt.

5. Archivierung

Da mit der betrieblichen Projektarbeit große Datenmengen anfallen, werden abgeschlossene Projekte verschlüsselt in zweifacher Ausführung auf Bänder archiviert und von den betreffenden Servern gelöscht. Der Zeitpunkt wird durch die Projektleiter festgesetzt.

Die Lagerung erfolgt jeweils unter Verschluss.

Vertrauliche Daten und sehr vertrauliche Daten werden bei der Archivierung nicht berücksichtigt sondern sicher gelöscht.

6. pslsrv10 und mobile Raids

Filmmaterial wird auf zwei jeweils gespiegelten (Raid-1) und verschlüsselten (AES 256) mobilen Raids getrennt (verschiedene Transport-Routen und -Mittel) vom Dreh zur Verarbeitung zu Parasol Island transportiert. Hier wird der Inhalt der Raids auf den zentralen Datenserver pslsrv10 kopiert. Ein Raid wird bis zum Projektende im 2. Serverraum in einem anderen Brandabschnitt als hochverfügbare Kopie gelagert.

7. Infrastruktur

Für die Datensicherung wird folgende Infrastruktur genutzt:

- Backupserver: pslsrv05
- Bandlaufwerke: 2x Neo Overland 4000 LTO 5
1x BDT LTO 6
1x Quantum Scalar i40 LTO 5
- Bänder: LTO 2 / LTO 3 / LTO 5 / LTO 6



Parasol Island

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 „Archiware P5“ eingesetzt.

8. 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 der Anwendungsdaten kann deshalb nicht genannt werden. Der Beginn der inkrementellen Sicherungen ist täglich um 20:00 Uhr. Die Backupinfrastruktur ist so ausgelegt, dass am darauffolgenden Tag spätestens um 09:00 alle Daten gesichert wurden.

9. Rekonstruktion von Daten

Ohne Datensicherung besteht keine Möglichkeit, zerstörte oder gelöschte Datenbestände wieder zu rekonstruieren.

Prinzipiell werden alle spezifizierten 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 1 Tage betragen. Jedoch verfügt der zentrale Datenserver pslsrv10 über eine Snapshot-Funktion, die in solchen Fällen die Verlustquote deutlich reduzieren kann.

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.

10. Rekonstruktionszeiten

Die Wiederherstellungsdauer von Daten hängt im Wesentlichen von der Anzahl und der Größe der zu rekonstruierenden Dateien ab.

11. Datensicherheit

Die Tape-Library ist so dimensioniert, dass die letzten 60 Tage Backup-Datensicherung jederzeit abgerufen werden können. Die Magnetbänder für diese inkrementelle Sicherung müssen niemals das geschützte Gehäuse des Bandlaufwerks verlassen. Die geschriebenen Daten werden AES 256Bit verschlüsselt. Die Tape-Library befindet sich in einem anderen Brandabschnitt als die zu sichernden Daten. Zugriff haben nur die Mitarbeiter, zu deren Aufgaben die Datensicherung gehört.



12. Kontrollen der Datensicherungen

Anhand von Protokollen der Sicherungssoftware wird wöchentlich 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 spätestens alle vier Wochen, mit zufällig ausgesuchten Daten, durchgeführt.

13. Sicherung von Dateien der Benutzer

Alle Mitarbeiter/Innen müssen sämtliche dienstliche Daten auf den spezifizierten Netzlaufwerken ablegen, da nur die Inhalte dieser Laufwerke auch bei der Datensicherung mitberücksichtigt werden. Weiterhin sind Mitarbeiter/Innen dazu angehalten in allen Anwendungen angemessene Einstellungen für ein automatisches Sichern Ihrer Arbeit vorzunehmen.

Lokale Dateien sollten für den Betriebsablauf nur in Form von Systemdaten vorliegen. Es liegt in der Verantwortung des Benutzers, diese Daten selbst zu sichern.