

# Backup & Wiederherstellung

- [Backup- & Restore-Plan](#)
- [Restore-Testprotokoll - Vorlage](#)
- [BackUp - Produktivsysteme](#)

# Backup- & Restore-Plan

# Backup- & Restore-Plan

System	RPO	RTO	Verfahren	Testintervall	Letzter Test/Nachweis
Fileserver	4h	8h	{{Tool}}	Quartal	{{Datum/Link}}
AD	4h	8h	System State	Halbjahr	{{Datum/Link}}

**Offsite/Immutable:** {{ja/nein, Speicherort}}

**Restore-Tests:** Vorgehen, Abnahmekriterien, Protokollvorlage

# Restore-Testprotokoll – Vorlage

## Restore-Testprotokoll

Datum	System	Umfang	Ergebnis	Prüfer	Maßnahmen
-------	--------	--------	----------	--------	-----------

# BackUp - Produktivsysteme

Dokumentation

## Backup-Dokumentation (3-2-1)

Organisation: **IT-TEAM** · Version: **1.1** · Gültig ab: **07.10.2025** · Zeitzone: **Europe/Berlin**

Eigentümer: **IT-Leitung**

Kontakt: Team-Channel IT it@...

## Inhalt

1. [Ziel & Geltungsbereich](#)
2. [3-2-1 Prinzip](#)
3. [Backup-Ziele](#)
4. [Backup-Quellen & Ziele](#)
5. [Sicherungsarten & Zeitplan](#)
6. [Aufbewahrungsrichtlinien](#)
7. [QNAP-Ordnerstruktur](#)
8. [Rollen & Verantwortlichkeiten](#)
9. [Zugangsdaten & Schlüsselmaterial](#)
10. [Monitoring, Berichte & Eskalation](#)
11. [Wiederherstellung \(Restore\)](#)
12. [Restore-Test-Checkliste](#)
13. [Verfahren \(operativ\)](#)
14. [Sicherheit & Compliance](#)
15. [Kapazitäts- & Lifecycle-Management](#)
16. [Änderungskontrolle & Versionierung](#)
17. [Anhänge](#)

# Ziel & Geltungsbereich

Diese Dokumentation beschreibt Aufbau, Betrieb und Kontrolle der Backup-Strategie nach dem 3-2-1-Prinzip für die IT-Infrastruktur. Sie gilt für alle produktiven Systeme (Server, Dienste, Konfigurationen, Shares) der Organisation.

## 3-2-1 Prinzip (umgesetzt)

- **3 Kopien:** Produktivdaten + mindestens zwei unabhängige Sicherungskopien.
- **2 Medientypen/Orte:** QNAP-NAS (2 Systeme), externe Wechselmedien (3 Festplatten), Windows-Backup-Server (Veeam), Linux-Backup-Server (immutable).
- **1 Kopie extern/offline:** Wöchentliche Sicherung auf externe Festplatten (Wechselbetrieb).

## Backup-Ziele

- **RPO:** ≤ 24 h (tägliche Sicherungen).
- **RTO:** systemabhängig; Priorität laut Notfallbetrieb (siehe Ordnerstruktur QNAP).
- **Integrität & Unveränderlichkeit:** Linux-Backup-Server mit immutable-Speicher.

## Backup-Quellen & Ziele

### Quellen (Beispiele)

- Active Directory (Domänencontroller)
- Applikations-/Applikation-Server
- File-Server (Shares, Berechtigungen)
- Terminalserver
- Hilfssysteme: Printserver, Schließanlage

# Ziele / Speicherorte

1. **QNAP-NAS A & QNAP-NAS B**  
Primäre NAS-Ziele für tägliche Sicherungen; Ordnerstruktur zur Priorisierung.
2. **Windows-Server mit Veeam**  
Führt Sicherungs- und Aufbewahrungslogik aus.
3. **Linux-Server (immutable)**  
Unveränderlicher Ziel-Datenspeicher; aktuell ohne automatische Löschung.
4. **Externe Wechselmedien (3× HDD)**  
Wöchentliche Offline-Rotation (extern lagerbar).

# Sicherungsarten & Zeitplan

- **Tägliche Sicherungen:** alle Systeme, Start täglich 20:00.
- **Wöchentliche Sicherung auf externes Medium:** Rotation über 3 Festplatten (HDD1, HDD2, HDD3).
- **Monatliche Vollsicherung:** zusätzlich zu den täglichen Inkrementen/Differentials.
- **Jährliche Vollsicherung (Jahresarchiv):** Langzeitaufbewahrung.

Zeitfenster mit Wartungsfenstern/Batch-Jobs abstimmen, um Lastspitzen zu vermeiden.

# Aufbewahrungsrichtlinien

## Standard (alle Server außer Linux-immutable)

- 7 Tage tagesaktuelle Wiederherstellungspunkte
- 1× pro Monat: Vollbackup (Monatsstand)
- 1× pro Jahr: Vollbackup (Jahresstand)

## Linux-Backup-Server (immutable)

- Aktuell ohne Löschung (unbegrenzte Aufbewahrung)
- Kapazität regelmäßig prüfen; perspektivische Lifecycle-Policy definieren (z. B. GFS/Objekt-Lock-Retention)

# QNAP-Ordnerstruktur (Zielablage)

```
/Backups
├─ Notfallbetrieb
│  ├─ ActiveDirectory
│  ├─ ApplikationServer
│  └─ FileServer
├─ Hilfssysteme
│  └─ Printserver
└─ Schliessanlage
    └─ Terminalserver
```

**Bedeutung:** Notfallbetrieb (höchste Priorität), Hilfssysteme (unterstützende Dienste), Terminalserver (Benutzer-Sitzungen).

## Rollen & Verantwortlichkeiten

- **IT-Leitung:** Freigabe der Richtlinie, Budget & Kapazität.
- **Backup-Admin (Veeam/Storage):** Job-Design, Aufbewahrungen, Rotationen, Monitoring, Berichte.
- **System-Owner (Workloads):** Funktionsprüfung der Anwendungen, Teilnahme an Restore-Tests.
- **Security/Compliance:** Immutable-Schutz, Zugriffskontrollen, Audit-Bereitschaft.

## Zugangsdaten & Schlüsselmaterial

**Ablage:** Passbolt. **Prinzip:** Need-to-Know, Vier-Augen-Prinzip. **Achtung:** Keine Zugangsdaten in dieser Dokumentation hinterlegen.

## Monitoring, Berichte & Eskalation

- Statusberichte werden **täglich** an die **IT-Mitarbeiter** gesendet und **täglich geprüft**.

- Prüfkriterien: Job-Erfolg/Fehler, Dauer/Throughput, Änderungsrate, Kapazität, Replikations-/Immutable-Status.
- Eskalation: ITSM-Ticket, On-Call/Backup-Admin, Sofortmaßnahmen bei Notfallbetrieb.

# Wiederherstellung (Restore)

- Regelmäßige Tests: **vierteljährlich** (quartalsweise) Stichproben-Restores.
- Umfang: mind. je ein System aus Notfallbetrieb, Hilfssysteme, Terminalserver – inkl. Anwendungsprüfung.
- Dokumentation: Ergebnisprotokoll mit RTO/RPO-Istwerten, Screenshots/Logs, Lessons Learned.
- Ad-hoc-Restores: nach Bedarf; dokumentierter Change.
- **Technische Durchführung:** siehe separate Dokumentation „Restore-Prozessbeschreibung“.

# Restore-Test-Checkliste

Diese Checkliste dient der strukturierten Durchführung und Dokumentation der vierteljährlichen Restore-Tests. Der technische Ablauf ist in einer separaten Dokumentation beschrieben.

#	Prüfschritt	Beschreibung	Verantwortlich	Ergebnis / Bemerkung
1	Testauswahl	Auswahl der Systeme gemäß Rotation (Notfallbetrieb, Hilfssysteme, Terminalserver)	Backup-Admin	
2	ITSM-Ticket	Anlegen des Restore-Tickets im ITSM inkl. Scope und Risiken	Backup-Admin	
3	Restore durchführen	Durchführung gemäß Prozessbeschreibung (isolierte Testumgebung/Ersatzsystem)	System-Owner / Backup-Admin	
4	Funktionstest	Dienste starten, AD-Login, Datenkonsistenz, Applikationschecks	System-Owner	

#	Prüfschritt	Beschreibung	Verantwortlich	Ergebnis / Bemerkung
5	RTO/RPO erfassen	Ist-Werte dokumentieren (Start/Ende, Wiederanlaufzeit, Datenstand)	Backup-Admin	
6	Protokoll	Restore-Protokoll inkl. Screenshots, Logs, Hash-/Integritätschecks	Backup-Admin	
7	Review & Abnahme	Fachlicher/technischer Review, Abnahme durch IT-Leitung	IT-Leitung	
8	Lessons Learned	Anpassungen an Jobs, Retention, Kapazität, Runbooks ableiten	Backup-Admin / IT-Leitung	

# Verfahren (operativ)

## 1) Täglicher Betrieb (Start 20:00)

1. Veeam-Jobs starten; Linux-Immutable-Targets online.
2. Fortschritt/Logs überwachen.
3. Nach Lauf: Statusbericht erzeugen/versenden; Team prüft bis nächsten Arbeitstag 10:00.

## 2) Wöchentliche Offline-Rotation (3× HDD)

1. Aktive HDD abkoppeln → sicher lagern (Offsite/Brandschutz empfohlen).
2. Nächste HDD anschließen/mounten.
3. Integritätsprüfung (SMART/FS-Check/Hash-Checks, sofern verfügbar).
4. Backup planmäßig laufen lassen; Rückmeldung im Wochenreport dokumentieren.

## 3) Monatliche & jährliche Vollbackups

- Per Veeam-Zeitplänen/Policies.
- Erstellung und Kopie auf sekundäre Ziele überprüfen (QNAP B / Immutable).
- Jahressätze gesondert kennzeichnen.

## 4) Restore-Test (quartalsweise)

1. Auswahl Testobjekte nach Kritikalität/Rotation.
2. Wiederherstellung in isolierter Testumgebung oder auf Ersatzsystem.
3. Funktions-/Integritätsprüfung mit Fachbereichen.
4. Protokollierung im Testregister gemäß Checkliste.

## Sicherheit & Compliance

- Immutable-Ziel schützt gegen Verschlüsselung/Manipulation.
- Rollenbasierte Zugriffe, Protokollierung aktiv.
- Netzsegmentierung des Backup-Pfads; gehärtete Admin-Workstations.
- Malware-/Checksum-Prüfungen vor/nach Backup-Fenster (wenn verfügbar).
- Datenschutz & Datenminimierung beachten.

## Kapazitäts- & Lifecycle-Management

- QNAP/Windows/Immutable-Speicher wöchentlich prüfen (Trend, Füllstand, Dedupe/Kompression).
- Alerting bei Schwellwerten (z. B. 80/90/95 %).
- Linux-Immutable: aktuell ohne Löschung → Kapazitäts-Forecast und ggf. künftige Retention-Policy definieren.

## Änderungskontrolle & Versionierung

- Änderungen an Jobs, Zeiten, Aufbewahrung, Zielen nur per Change-Prozess (RFC).
- Dokumentation versionieren; Changelog pflegen.

# Changelog

- **1.1 (07.10.2025):** Ergänzung Restore-Test-Checkliste.
- **1.0 (07.10.2025):** Erstdokumentation basierend auf aktuellem Betriebsstand.

# Anhänge

- A1: Verteiler „IT-Mitarbeiter“ für Statusberichte.
- A2: Passbolt-Eintrag (Ordner/Gruppe) für Backup-Zugänge (ohne Details in diesem Dokument).
- A3: Restore-Testprotokoll-Vorlage (RTO/RPO-Checkliste).

© IT-TEAM · Dieses Dokument enthält betriebskritische Informationen. Interne Verwendung.