

NovaTech Solution

Standard Operating Procedure

Backup and Disaster Recovery (BDR) Procedures

Document Information: SOP-BDR-001

Version: 1.0

Last Updated: April 2, 2025

Owner: IT Operations Team

Confidentiality Level: Internal Use Only

Overview

This Standard Operating Procedure (SOP) establishes the processes for backing up, protecting, monitoring, and recovering NovaTech Solutions' critical systems and data. It defines backup schedules, storage locations, retention policies, recovery objectives, and disaster recovery procedures to support business continuity.

1. Purpose

The purpose of this SOP is to define the standardized procedures for performing system backups and executing disaster recovery operations to ensure business continuity and data integrity.

2. Scope

The SOP applies to all IT-managed systems and data environments across:

- Physical servers (on-premises)
- Virtual machines (VMware, Hyper-V)
- Cloud platforms (AWS, Azure, Google Cloud)
- SaaS platforms (Microsoft 365, Salesforce)
- End-user devices (as applicable)

3. Prerequisites

Before performing backup or recovery tasks:

- Administrative access verified
- Backup infrastructure operational
- Storage capacity validated
- Encryption keys available
- Incident tickets documented when applicable

4. Roles & Responsibilities

Role	Responsibilities
IT Infrastructure Lead	Oversees the overall Backup and Disaster Recovery (BDR) strategy; approves backup policies, retention schedules, and disaster recovery plans; ensures compliance with internal governance and regulatory standards (ISO 27001, SOC 2, HIPAA where applicable); coordinates with senior leadership during high-impact incidents.
Backup Administrator	Configures, schedules, and maintains all backup jobs across on-premises and cloud environments; monitors daily backup success/failure reports; performs backup validation and test restores; ensures backup integrity, availability, and performance; manages backup software platforms (e.g., Veeam, RMAN).
Security Analyst	Ensures all backup data is encrypted in transit and at rest; monitors backup environments for unauthorized access or anomalies; enforces identity and access management (IAM) policies including MFA; conducts vulnerability assessments and supports incident response related to data compromise.
Disaster Recovery (DR) Coordinator	Leads execution of disaster recovery procedures during outages or critical incidents; activates DR plan based on severity classification; coordinates recovery teams across infrastructure, applications, and security; maintains DR runbooks and ensures regular DR testing and documentation updates.
Application Owners	Identify mission-critical applications and data dependencies; define recovery priority requirements (RTO/RPO) for assigned

	systems; validate application functionality following restoration; confirm data integrity and business readiness post-recovery.
Database Administrator (DBA)	Manages database backup and recovery processes (full, incremental, and log-based backups); ensures database consistency and integrity during restoration; performs point-in-time recovery when required; monitors database performance and storage utilization.
Cloud Systems Engineer	Manages backup and replication of cloud workloads (AWS, Azure, GCP); ensures proper configuration of cloud storage tiers and cross-region replication; supports cloud-based disaster recovery failover and failback procedures; optimizes cloud backup cost and performance.
IT Service Desk / Support Team	Serves as the first point of contact during incidents; logs and escalates backup or system failure tickets; communicates status updates to end users; supports verification of restored services from a user perspective.
Compliance Officer (IT Governance)	Ensures backup and disaster recovery procedures meet regulatory, legal, and contractual requirements; reviews audit logs and retention compliance; participates in annual audits and policy reviews; validates adherence to data governance standards.

5. Definitions

- **RTO (Recovery Time Objective):** Maximum acceptable downtime (e.g., 4 hours)
- **RPO (Recovery Point Objective):** Maximum acceptable data loss measured in time (e.g., 15 minutes)
- **Failover:** Switching to a standby database or system in case of failure
- **Hot Site:** Fully equipped alternate site with real-time data replication
- **Snapshot:** Point-in-time image of a system or VM for quick rollback

6. Disaster Recovery

6.1 Triggering Events

System Type	Backup Type	Frequency	Retention
-------------	-------------	-----------	-----------

File Servers	Full + Incremental	Daily at 2 AM	30 days
Databases (SQL, Oracle)	Transaction Log + Full	Logs every 15 min; full daily at 1 AM	60 days
Virtual Machines	Snapshots	Hourly, Daily, Weekly	14 days (hourly), 90 days (weekly)
Microsoft 365 (Mail, OneDrive, Teams)	Cloud Backup	Daily	1 year
Configuration Files	Full	Weekly	1 year
Archive Systems	Full (cold storage)	Monthly	7 years

6.2 Backup Environment/Systems

System	Tool	Primary Storage	Offsite/Cloud
On-Prem Servers	Veeam Backup & Replication	NAS + External Disk Vault	AWS S3 Glacier + Azure Blob
Databases	SQL Server Agent, Oracle RMAN	SAN Volume	Azure Backup Vault
Office 365	Veeam O365 Plugin	Azure Storage Account	Same Region & Cross-region
VMs (VMware/Hyper-V)	Veeam + vSphere	SAN + NFS	AWS S3 + Azure

6.3 Restoration Matrix

Security Control	Description
Encryption	All backups are encrypted in transit (TLS 1.2+) and at rest (AES-256)
Access Control & Monitoring	Backup storage is access-controlled and monitored via SIEM

Authentication	MFA required for all administrative access to backup systems
Vulnerability Management	Regular vulnerability scans are conducted on backup infrastructure

6.4 Monitoring & Reporting

Monitoring Control	Description
Real-time Monitoring	Backup jobs are monitored in real-time through Veeam One Dashboard
Daily Reporting	Daily success/failure reports are emailed to the IT Ops team
Monthly Reporting	Monthly health check and report is presented to IT leadership
Alerting & Escalation	Alerts are configured for missed or failed jobs (threshold: 1 failure triggers escalation)

6.5 DR Activation Procedures

Triggering Event	Description
Data Center Outage	Complete or partial data center outage
Cybersecurity Breach	Cybersecurity incident such as ransomware
Natural Disaster	Events such as fire, flood, or earthquake
Cloud Service Disruption	Cloud outage exceeding RTO threshold
Human Error	Major mistakes such as accidental deletion or critical system failure

6.6 DR Response Phases

Phase	Action Steps
Detection & Escalation	Detect outage/incident via monitoring tool and Notify IT Director, CIO, Legal

Assessment	Determine affected systems and scope and classify disaster level (Minor, Major, Critical)
Activation	Intitiate DR plan per priority matrix and mobilize DR team
Restoration	Prioritize recovery per critical systems (ERP, CRM, Mail, Web) and restore from most recent clean backups
Validation	Perform functional, integrity, and security tests post-restore

6.7 Priority Restoration Matrix

System	Priority	RTO	RPO
Email (Microsoft 365)	High	2 hours	15 minutes
ERP System	Critical	1 hour	5 minutes
File Server	Medium	6 hours	1 hour
Website	High	2 hours	30 minutes
HR System	Low	24 hours	4 hours

7. Diagram

flowchart TD

A[Systems & Data Sources] --> B[Backup Jobs Executed]

B --> C[Validation & Integrity Checks]

C --> D[Backup Storage Repositories]

D --> E[Monitoring & Alerting via Veeam One]

E --> F{Incident Detected?}

F -- No --> G[Normal Operations Continue]

F -- Yes --> H[Assess Severity]

H --> I{Disaster Recovery Required?}

I -- No --> J[Restore from Backup / Minor Recovery]

I -- Yes --> K[Activate DR Plan]

K --> L[Failover to DR Environment]

L --> M[Restore Critical Systems by Priority]

M --> N[Validation & Testing]

N --> O[Return to Normal Operations]

8. Compliance & Audit

- Adheres to ISO 27001, NIST SP 800-34, SOC 2, and HIPAA (as applicable)
- All backup and DR logs retained for 1 year
- Internal audit of BDR procedures conducted annually
- External audit readiness supported by audit trails, restore logs, test results

9. Review & Maintenance

- Quarterly review of SOP content, backup schedules, retention policies
- Annual full plan update approved by IT Governance Board
- Change Control: All edits to SOP are version-controlled and reviewed by Compliance Officer

10. Documentation & References

- Business Continuity Plan (BCP)
- Data Classification Policy
- Cloud Security Policy
- Vendor SLA documents for backup and cloud storage
- [Backup Software] Admin Guide
- DR Runbook Checklist

11. Approval

Name	Title	Status	Date
Janice Smith	IT Manager	Approved	February 11, 2025
Lee Davis	CIO	Approved	March 28, 2025
Sandra Olive	Compliance Officer	Approved	January 17, 2025

12. Revision History

Version	Date	Author	Description
1.0	2025-04-02	IT Operations Team	Initial release