📄 Document 4

Southstar Tech Solutions

Data Retention & Backup Policy

Version: 1.0
Effective Date: January 2026
Owner: IT Operations & Compliance

---

1. Purpose

This policy defines how Southstar Tech Solutions stores, protects, retains, and disposes of company data to ensure availability, integrity, and compliance.

---

2. Scope

Applies to:

- All company data (customer, employee, operational)
- On-premise systems
- Cloud services (AWS & Azure)
- End-user devices

---

3. Data Classification

Level	Description
Public	Non-sensitive information
Internal	Business-use information
Confidential	Sensitive business data
Restricted	Highly sensitive regulated data

---

4. Data Retention Guidelines

Data Type	Retention Period
System Logs	1 year
Financial Records	7 years
Security Incident Records	5 years
Employee Records	Duration of employment + 3 years
Backup Archives	90 days rolling

---

5. Backup Procedures

- Daily incremental backups
- Weekly full backups
- Backups stored in secure cloud vault
- Veeam used for backup management

---

6. Backup Security

- Backup data encrypted at rest
- Access limited to authorized IT staff
- MFA required for backup console

---

7. Disaster Recovery

- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 24 hours
- Quarterly recovery testing required

---

8. Data Disposal

When retention period ends:

- Data securely deleted
- Storage media wiped or destroyed
- Compliance review conducted

---

9. Compliance Alignment

This policy aligns with:

- NIST Data Protection guidelines
- ISO 27001 Annex A.12
- GDPR data minimization principles

---

10. Tools Used

Tool	Purpose
Veeam	Backup management
AWS S3 Glacier	Archive storage
Splunk	Log retention

---

11. Review Cycle

Reviewed annually or when regulatory changes occur.