Backup & Recovery SOP

1. Purpose

Define the standard procedures to protect business data from accidental deletion, corruption, or ransomware incidents.

2. Scope

This SOP applies to:

- Business data in C:\CompanyData
- Backup destinations: Manual (C:\Backups_Manual), Script (C:\DailyBackup)

3. Backup Methods

Method	Description	Frequency	Location
Manual Backup	User-initiated copy	Daily	C:\Backups_Manual
Automated Script Backup	PowerShell-based	Daily	C:\DailyBackup

4. Manual Backup Procedure

1. Navigate to C:\CompanyData
2. Copy folder to C:\Backups_Manual
3. Verify folder size and files
4. Log activity (optional)

5. Automated PowerShell Backup

- Script path: P5_Backup_Recovery\scripts\backup.ps1
- Run with:
  `powershell -ExecutionPolicy Bypass -File .\backup.ps1`

Outputs:

- Timestamp backup folder
- Log file: C:\DailyBackup\backup_log.txt

6. Recovery Procedures

6.1 Accidental Deletion

1. Identify missing file
2. Retrieve latest version from backup folder
3. Restore to original location

4. Verify integrity

6.2 Ransomware Incident Simulation

1. Identify encrypted or renamed files
2. Remove malicious note/encrypted file
3. Restore clean copy
4. Validate data correctness

---

7. Testing & Validation

- Monthly backup restore testing
- Log verification
- Compare file hash (if applicable)

---

8. Documentation & Logging

- Logs stored at: C:\DailyBackup\backup_log.txt
- Evidence and screenshots stored in `/screenshots`
- Official documents stored in `/documents` and `/assets`