Network Server Backup Policy Example

1. Purpose

The purpose of this policy is to establish the guidelines for backup and restoration of data on network servers to ensure data integrity, availability, and security.

2. Scope

This policy applies to all servers, systems, and personnel responsible for data backup and recovery within the organization.

3. Policy Statements

1. All critical server data must be backed up according to the schedule defined below.
2. Backups must be stored securely to protect them from unauthorized access, theft, or damage.
3. Backups shall be tested periodically to ensure data can be reliably restored.
4. Personnel must document and follow standardized backup and restoration procedures.
5. Retention periods for backups must comply with legal, regulatory, and business requirements.

4. Backup Schedule

Data Type	Frequency	Retention Period	Storage Location
System Configuration Files	Daily	30 Days	On-site & Off-site
User Data	Daily	90 Days	On-site & Off-site
Database Files	Hourly Incremental, Daily Full	30 Days	Off-site

5. Restoration

Restoration procedures must be documented and accessible to authorized personnel. In the event of data loss or corruption, restoration shall occur as quickly as possible to minimize downtime.

6. Roles and Responsibilities

- **IT Administrators:** Perform regular backups, monitor backup logs, test restoration, and ensure policy compliance.
- **Data Owners:** Identify critical data and communicate backup requirements.
- **Management:** Provide resources and support for backup operations.

7. Policy Review

This policy will be reviewed annually or after significant changes to systems or processes.

8. Exceptions

Any exceptions to this policy must be approved in writing by the IT Manager.