Cloud Storage Backup Policy Template

1. Purpose

This policy defines the requirements and procedures for backing up data stored in cloud storage solutions to ensure its integrity, availability, and recoverability.

2. Scope

This policy applies to all organizational data stored in company-approved cloud storage platforms, including but not limited to shared files, databases, and application data.

3. Roles and Responsibilities

Role	Responsibility
IT Administrator	Implements and reviews the backup policy; monitors backup jobs and performs restores as necessary.
Department Managers	Ensure department data follows backup procedures.
All Users	Store data in approved cloud solutions to guarantee inclusion in backups.

4. Backup Procedures

1. Backups will be scheduled automatically on a daily basis.
2. Use provided tools by the cloud vendor or approved third-party solutions.
3. Replicate backups to a geographically separate region, if supported.
4. Test backup restoration bi-annually and document results.

5. Retention Policy

- Daily backups retained for 14 days
- Weekly backups retained for 3 months
- Monthly backups retained for 1 year

6. Data Security and Encryption

All backups must be encrypted in transit and at rest using industry-standard encryption methods.

7. Monitoring and Reporting

- Backup logs will be reviewed weekly.
- Alerts for failed backup jobs will be sent to IT Administrators.

8. Exceptions

Any exceptions to this policy must be documented and approved by the IT Manager.

9. Review and Update

This policy will be reviewed annually and updated as necessary to reflect changes in technology and organization requirements.

10. Approval

Name	Title	Date	Signature