SOP: Backup and Disaster Recovery Processes

This SOP details the **backup and disaster recovery processes** essential for protecting critical data and ensuring business continuity. It includes regular data backup schedules, secure storage methods, verification of backup integrity, disaster recovery planning, roles and responsibilities during recovery, and procedures for restoring systems and data after an incident. The goal is to minimize data loss and downtime by implementing robust and reliable backup and recovery strategies.

1. Purpose

To outline the requirements and procedures for backing up organizational data and recovering critical systems and information in the event of data loss or disaster.

2. Scope

This SOP applies to all IT systems and data managed by [Organization Name], including onsite, offsite, and cloud-based resources.

3. Definitions

- **Backup:** A copy of data maintained for restoring in case of data loss.
- **Disaster Recovery:** The process of restoring systems and data after a disruption or catastrophic event.
- **Recovery Point Objective (RPO):** The maximum acceptable amount of data loss measured in time.
- **Recovery Time Objective (RTO):** The maximum acceptable length of time to restore systems and operations.

4. Roles and Responsibilities

Role	Responsibilities
IT Manager	Oversee backup and recovery processes; review and update SOP as necessary.
System Administrators	Execute backup, integrity checks, disaster recovery drills, and restorations.
All Staff	Report incidents of data loss or corruption; follow prescribed procedures.

5. Procedures

5.1 Backup Schedule

- **Daily:** Incremental backups of critical data.
- **Weekly:** Full backups of defined systems and storage.
- **Monthly:** Full archival backup, securely stored offsite or in the cloud.

5.2 Secure Storage

- Encrypt all backup data at rest and in transit.
- Store backups in physically and logically secure locations, separate from production systems.
- Maintain at least one offsite or cloud-based backup copy.

5.3 Backup Verification

- Perform integrity checks after each backup job.
- Log and review backup jobs for errors and ensure resolution of issues.
- Test restore procedures from backups monthly on a non-production system.

5.4 Disaster Recovery Process

1. **Incident Detection:** Identify and confirm data loss or system failure event.
2. **Assessment:** Evaluate extent and impact of incident, initiate disaster recovery plan.
3. **Notification:** Notify stakeholders and relevant response teams.

4. **Restoration:** Restore affected systems and data from backups based on RPO and RTO requirements.
5. **Validation:** Verify integrity of restored systems and data before resuming operations.
6. **Review:** Document incident, actions taken, and lessons learned.

6. Documentation & Review

- Maintain logs of all backup and restore operations.
- Review and test disaster recovery plan **at least annually** or after significant system changes.

7. References

- Backup and Restore Policy
- Disaster Recovery Plan
- Incident Response Procedures

8. Revision History

Date	Version	Description of Change	Author
[YYYY-MM-DD]	1.0	Initial SOP issued	[Name]