Data Backup Policy

Description: This policy outlines the procedures, frequency, and storage methods for backing up organizational data to ensure its availability and protection.

Category: IT & Security

1. Purpose

To ensure that all critical organizational data is regularly backed up, securely stored, and recoverable in the event of data loss, system failure, or disaster.

2. Scope

This policy applies to all systems, servers, databases, and user data managed or owned by the organization.

3. Backup Frequency

- Daily backups are required for critical systems and databases.
- Weekly backups for less critical data and archive systems.
- Backups must be scheduled automatically and monitored for successful completion.

4. Backup Storage Locations

- Backups must be stored in at least two different locations: one onsite (e.g., local server) and one offsite (e.g., cloud storage or external facility).
- Offsite backups must be encrypted and securely transmitted.
- Access to backup storage must be limited to authorized personnel only.

5. Retention Periods

- Daily backups must be retained for 7 days.
- Weekly backups must be retained for 4 weeks.
- Monthly backups must be retained for 12 months.
- Archived backups of critical data may be retained for longer based on legal or regulatory

requirements.

6. Backup Testing and Validation

- Backups must be tested monthly to ensure data integrity and recoverability.

- Any failed backups must be logged, investigated, and resolved immediately.

7. Roles and Responsibilities

- The IT department is responsible for implementing, monitoring, and reviewing backup procedures.

- All staff must report any data loss or backup-related issues immediately to IT.

8. Policy Review

- This policy must be reviewed and updated annually or following major changes in infrastructure or operations.

Created by: Admin

Published under: Policy Management System