# Backup Strategy

* 1. **Backup Types**

1. **Full Back up:** Complete backup of the entire database and application data.
2. **Incremental Backup:** Backup only changes since the last backup (full or incremental).
3. **Differential Backup:** Backup changes since the last full backup. (Work on)

# Backup Frequency

## Database Backup:

* Full backups weekly (e.g., Sunday night). 
* Differential backups daily.
* Transaction log backups every 15 minutes (for Point-in time recovery).

# Backup Storage

* Backups should be stored in geographically separate locations (onsite and offsite/cloud storage).
* Use encryption for all backups to protect data confidentiality.
* Maintain at least 4 weeks of backup history for daily backups and 3 months for full backups.

# Backup Procedures

* 1. **Database Backup**
* Utilize appropriate PostgreSQL backup tools:
  +  Full backups using pg\_dump or base backups via pg\_basebackup.
  +  Transaction log WAL) archiving enabled for point-in-time recovery.
* Verify backup integrity by periodic test restores.
* Automate backup jobs using pgAgent or similar scheduler with alerting on failures.

# Backup Verification

* Perform monthly restore tests to backup environments to validate backup reliability.  Monitor and log all backup activities with notifications for errors.

# Recovery Procedures

* 1. **Restore from Backup**
* Prioritize recovery based on system criticality: core modules first, auxiliary modules second.
* Use base backups with WAL logs for point-in-time recovery to a specific moment before failure.
* Document and review each recovery by performing validation checks of data integrity.
* Maintain recovery time objectives (RTO) and recovery point objectives (RPO) according to business needs (e.g., RTO ≤ 4 hours, RPO ≤ 15 minutes).

# Disaster Recovery

* In event of catastrophic failure, switch to offsite backup infrastructure.
* Maintain documented step-by-step disaster recovery plans accessible to all relevant personnel.
* Regularly update disaster recovery plans and conduct drills.

# Security and Compliance

* Secure backup media and restrict access to authorized personnel.
* Encrypt backups both in transit and at rest.
* Ensure compliance with relevant data protection regulations.

# Documentation and Reporting

* Maintain backup logs and recovery reports.
* Document all backup schedules, storage locations, and retention periods.
* Report backup status and recovery test outcomes to IT management monthly.