Liberty Wildlife DBA

Database Administration Processes:

The sanctuary will employ a **hybrid approach**:

1. **In-House DBA Team**:
    - Responsible for maintaining database structure, solving issues, and conducting compliance audits.
    - Benefits: Direct control over data, quicker issue resolution based on day-to-day operations.

2. **Cloud-Managed DBA Services**:
    - Handles backups, software updates, and security patches automatically.
    - Benefits: Reduces the workload for in-house staff team.

Why Use Cloud Services for This Database?

- The sanctuary expects rapid growth in both staff and animals. Cloud services can help optimize the performance of the projected growth without major hardware investments.
- Eliminates the need for expensive hardware upgrades and maintenance, which then reduces any financial strain.
- Cloud services simplify database administration, allowing the sanctuary to focus on its main mission and future goals.

Backup and Recovery Methods

1. **Backup Strategy**:
    - **Cold Backups**:
        - Full system backups done weekly when the database is offline.
    - **Hot Backups**:
        - Daily backups done while the database is running to avoid downtime.
    - **Incremental Backups**:
        - Smaller backups done several times a day to save changes since the last backup.
2. **Recovery Steps**:
    - If something goes wrong, we will:
        - Use backups to restore the data.
        - Use logs to reapply recent changes or fix any incomplete transactions.
    - **Examples**:
        - If the system crashes, we will roll back incomplete transactions and apply saved ones.
        - If a storage device fails, we will restore from the latest backup.

Security

1. **Physical Security**:
    - Keep servers in a locked, secure room with limited access to only authorized staff.
    - Add fire and flood protection.

2. **Access Control**:
    - Only let people see the data they need. For example:
        - Caretakers access animal info.
        - Financial staff access donation records.
    - Use strong passwords and multi-factor authentication

3. **Data Safety**:
    - Encrypt the data so it can't be read if it is stolen.
    - Regularly check and update software to protect against hackers.

4. **Auditing**:
    - Keep logs of who accesses the database and when.
    - Look for unusual/suspicious activity, such as failed logins or unexpected changes in data.

Monitoring and Maintenance

1. **Monitoring**:
    - Use tools to check for slow queries, low disk space, or unusual activity.
    - Set up alerts to warn the team about potential issues.

2. **Maintenance**:
    - Regularly update the database software.
    - Rebuild indexes to keep the database running smoothly.