IT Department Best Practices Guide - Database Architecture

Security:

All database security based at the user level. Each employee in the company has a domain authenticated username that they will use to access any database they have been authorized access to.

To restrict access to:

- *Database*: do not grant user access to the database.

- *Specific data in a database*: grant user access to all tables in the database, then revoke access to any tables holding restricted data.

Backups:

All database backup schedules should be set based on priority (Standard, Archived, Critical):

- *Standard*: Backup schedule is a full backup 1x per week.

- *Archive*: Backup schedule is a full backup 1x per month.

- *Critical*: Backup schedule is full backup 1x per week, incremental backup daily.

Storage:

All databases are given a standard partition of 1 GB by the server group. Ask users about the expected growth of data. Databases larger than or expected to exceed 10K rows of data in the next year should ask for a large partition space.

Databases are stored on spinning disk by default. In-memory storage is available, but only for data that requires higher level computations (advanced analytics, machine learning applications).

Data Ingestion:

Direct Feeds: If setting up a direct feed from another database, please ensure a functional username is created by IT security. This will ensure an expiring username does not cause a data flow error.

API: If working with API, please submit the API address and information to IT security for evaluation before proceeding.

ETL: ETL is the current best practice for working with flat files. If the flat file will be regularly updated, an automated ETL process can be set up.