Samuel Shelley
CPT 240 I01
Prof Carman
April 23, 2024

Project Milestone 4

Security Backup Policies

Steps for Backing Up the Database

1. Identifying necessary information to backup.
2. Address the appropriate location and type of storage.
3. Schedule appropriate times of backing up the database.
4. Ensure updated information is being transported and the information is secure.

Identify Necessary Information

The first reason to store backups of a database is because there is information that you do not want to lose to a natural disaster, ransomware attack, or mishap. Therefore, there is information that is necessary to include in the backups and may be some information that is unnecessary. One example of something that a company might not want to backup is daily ids of orders taking place at a fast-food restaurant. Even though this information is stored in a database, it may not be something you want to backup. The database stakeholders should agree and identify the necessary information for the database.

Addressing location and storage type

An organization should identify the location and type of storage that best fits business practices and database needs. This could include identifying whether to store a cloud backup or onsite backup, whether to store partial or full backups, and even what locations those backups will be stored geographically. A big part of security from damage comes down to what kind of environmental damage could occur. This is why the most secure database backups are stored in various places in a wide range of geographic locations.

Schedule Times for Backups

Finding the appropriate times and frequency of backups is important to every organization, and it is also unique to every organization. A database that stores less information but needs more security may be able to use a certain amount of storage and backup every week or two. A database that has more information and is less sensitive may use that same amount of storage and only have room to backup once a month. Schedules for backing up should be a priority for a business so that they can accomplish their tasks.

Ensure Backup is Secure

There should be routine checkups on the integrity of backups stored as well as the quality of reinstating that information when it is needed. The backups should be surveyed for inaccuracies or mishandling because this can be a common thing. IT professionals should take time to make sure that those backups keep their integrity. There should also be testing on data retrieval and retrieval management. How the information will be restored when a disaster does happen is important to work efficiently.