AC-2: ACCOUNT MANAGEMENT

Controls [a,b,c]:

The organization has categorized the four users into these roles. Each with their perspective, purpose and permissions.

- Database Administrator: Highest level of permissions on the server and database. Able to make any deletions, changes, modifications to the database.
  - This role is reserved for Administrators of the system
- Database Manager: Has full permissions only for the database.
  - This role is reserved for the managers who will be managing the database.
- Database Analyst: User who will be adding all necessary data.
- Normal Database User: Role with the most basic user who can view the tables and databases
  - This user does not necessarily have to be part of the organization.

Control [d]

Database Admin: Joshua Alaniz

Database Manager: Joshua Alaniz

Database Analyst: Joshua Alaniz

Normal Database User: N/A *anyone who wishes to view the database*

Control [e]

- All new account creation requests must be accepted by at least one Database Administrator or Database Manager.

Control [f]

NIST Risk Management Framework

- For monitoring accounts of the database it is the responsibility of <u>Database Administrator</u> and <u>Database Manager.</u>

Control [g]

- To create, enable, modify, disable, or remove accounts can only be done by <u>Database Administrator.</u>

Control [h]

- For accounts that no longer are used, have to be transferred, changing information systems becomes the responsibility of <u>Database Administrator</u>.

Control [i]

- Authorized access to information will be administered by the <u>Database Manager</u>.

Control [j]

- Compliance will be done by the <u>Database Manager</u>.

Control [k]

- <u>Database Administrator</u> will be responsible for the creation of reiusinng group credentials for when individual are removed.