**NIST-CONTROL AC-2 DOCUMENTATION**

**[ a, b, c ]** There are currently 4 roles created for the database system.

* **Database Administrator**, which has full access to both server and database functions
  + Only Database Admins should be given this role, is the condition for membership.
* **Database Manager**, which has full access to the database functions
  + Managers of Database projects would be given membership.
* **Database Designer**, which has access to all necessary creation and reverse engineering rights for databases
  + Those who are on the project and are solely developing and creating databases should be given membership within this role.
* **Database Basic Role**, which only has access to be able to see databases and their contents
  + Users who are either not in the project, or simply exploring the database, should be given this role. It is the most basic form of membership at the moment.

**[ d ]** Current Role membership is as follows for the project (roles assigned arbitrarily):

* **Database Administrator** – Piotr, Yuping
* **Database Manager** – Anthea, Sai
* **Database Designer** – Kemelbek, Magdalena, Zahid
* **Database Basic Role** – *None*

The role permissions are as follows:

* **Database Administrator:**
  + ALTER, ALTER ROUTINE, CREATE, CREATE ROLE, CREATE ROUTINE, CREATE TABLESPACE, CREATE TEMPORARY TABLES, CREATE USER, CREATE VIEW, DELETE, DROP, DROP ROLE, EVENT, EXECUTE, FILE, INDEX, INSERT, LOCK TABLES, PROCESS, REFERENCES, RELOAD, REPLICATION CLIENT, REPLICATION SLAVE, SELECT, SHOW DATABASES, SHOW VIEW, SHUTDOWN, SUPER, TRIGGER, UPDATE ON \*.\* TO 'Database\_Administrator' WITH GRANT OPTION
* **Database Manager**:
  + ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EVENT, INDEX, INSERT, LOCK TABLES, SELECT, SHOW DATABASES, SHOW VIEW, TRIGGER, UPDATE ON \*.\* TO 'Database\_Manager' WITH GRANT OPTION
* **Database Designer**:
  + ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE VIEW, INDEX, SHOW DATABASES, SHOW VIEW, TRIGGER ON \*.\* TO 'Database\_Designer'
* **Database Basic Role**:
  + SELECT, SHOW DATABASES, SHOW VIEW ON \*.\* TO 'Database\_Basic\_Role'

**[ e ]** Approval of account creation or role assigning must go through at least users of **Database Manager** role or above.

**[ f, g ]** Creation, Modification, or Removal of accounts or roles is only permitted to be done by **Database Administrators**. The same is applied to account monitoring and use.

**[ h ] Database Administrators** should routinely check whether or not accounts are being used by anyone. If an account has not been accessed, utilized, or modified in at least a month, it should be removed from the system. For time specific actions, refer to database **Time Stamps** applied from **AC-7** in the system.

**[ i ]** Access to the information system requires user approval by **Database Administrators**. This means any new users entering into the system (given accounts) must be given accounts by those of that role, and must be permitted to do so. Permission would require details as to intent within the project such as development, administrative, basic role, or others, and requires prior approval from the project group outside of the database to gain that permission.

**[ j ]** Account compliance and permission monitoring should only be available to **Database Administrators**. This entails checking back weekly to ensure roles are given only the required permissions to work on their respective sections of the project. Permissions should be in line with the policies from section **[ a, b, c]**.

**[ k ]** The removal and reissuing of credentials and accounts is to be done by **Database Administrators** in the event that project members either no longer require their current role permissions, or are leaving/being removed from the project. The process would entail tracing back everything attached to that person’s account, and removing connections before disabling/removing the account entirely.