|  |  |
| --- | --- |
| **Security, DCL, and Views (MIS 325) FA20**  Please fill out all blank parts of this template. | Name: Kyle Look Fong  UTEID: kal3565  Section: 04115 |

# 1. Access Control Matrix::

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Browser\_User | ContentCreator | CreditCard | Video |
| Member | I, U. Insert and Update so that the user can create their new accounts, select them, and update them. They should not have delete or insert so that they don’t access other user’s passwords and sensitive information. | I, U. The same rationale as browser\_user, especially because the browser\_user’s create their own content creator accounts. This should not include delete or select so they don’t delete entire rows or have access to individual’s sensitive information (e.g. Street address) | I, U. It should only be insert, as they should not be able to select or delete anybody else’s credit cards or update somebody else’s credit card. They should, however, be able to insert and update their own credit cards. | S, U, I, D. All should be granted as they should be able to select (e.g. in a search or comment), update their own videos, create their own videos, and delete their own videos |
| Account Manager | None. Account managers are responsible for working with content creators to upload videos. The browser user table includes non-content creators so it is best to not grant any access. | S. Only select due the fact that they should at least know some information about the content creator (like their tier level) but should not be able to alter the table. The account managers are responsible for uploading videos, not creating accounts. | None. The account managers are responsible for uploading videos with Content Creators. There is no reason for the account managers to have access to sensitive credit card information, especially with no correlation to the table. | S, I, U, D. Because they work with content creators to upload, they should be able to insert. Because they also help these creators manage videos, assuming manage can include delete videos, they should be able to update and delete videos as well. |
| Customer Service Rep | S, U, D. They should be able to have all privileges to the Brower\_User table as they assist with managing the account, including sensitive information. They should be able to delete an account if requested and select specific accounts from the able. They should not be able to insert as they help existing members. | S, I, U, D. They should be able to have all privileges to the Content Creator table as they assist with managing the account, including sensitive information. They should be able to delete an account if requested and select specific accounts from the able. They should be able to insert as existing members may want to become a content creator. | U. The customer service reps should only have access to Update the credit card table as it is a vital part of the member’s account. They should not be able to select every card in the table, they should not be able to delete cards, and they should not be able to insert cards as this is not their area of expertise. | None. They should not be able to access the Video table as they help members manage their account, not the videos they create. The video table doesn’t necessarily have sensitive info, but there is no need for customer service reps to have access. |

# 2-5. SQL tasks for this assignment:

1. Write the SQL code to create **roles** ofthe ***Member***, ***Account Manager,*** ***Customer\_Service\_Rep***

|  |
| --- |
| **Enter code here**  CREATE ROLE Member IDENTIFIED BY member\_password;  CREATE ROLE AccountManager IDENTIFIED BY a\_manager\_password;  CREATE ROLE CustomerServiceRep IDENTIFIED BY rep\_password; |

1. Write the SQL code to **Grant** the appropriate (object) **privileges** to the ***Member***, ***Account Manager,*** ***Customer\_Service\_Rep***

|  |
| --- |
| **Enter code here**  --Member Privileges  GRANT INSERT, UPDATE  ON Browser\_User  TO Member;  GRANT INSERT, UPDATE  ON ContentCreator  TO Member;  GRANT INSERT, UPDATE  ON CreditCard  TO Member;  GRANT ALL  ON Video  TO Member;  --Account Manager  GRANT SELECT  ON ContentCreator  TO AccountManager;  GRANT ALL  ON Video  TO AccountManager;  --Customer Service Rep  GRANT SELECT, UPDATE, DELETE  ON Browser\_User  TO CustomerServiceRep;  GRANT ALL  ON ContentCreator  TO CustomerServiceRep  GRANT UPDATE  ON CreditCard  TO CustomerServiceRep |

1. Write the SQL code to **Revoke** all the **privileges** from the ***Member***, ***Account Manager,*** ***Customer\_Service\_Rep***

|  |
| --- |
| **Enter code here**  --Account Manager  REVOKE ALL  ON ContentCreator  TO AccountManager;  REVOKE ALL  ON Video  TO AccountManager;  --Customer Service Rep  REVOKE ALL  ON Browser\_User  TO CustomerServiceRep;  REVOKE ALL  ON ContentCreator  TO CustomerServiceRep  REVOKE ALL  ON CreditCard  TO CustomerServiceRep |

1. Customer Service Reps should only be able to view billing information from the CreditCard table. They should not be able to see the card\_id, card number, card type, and security code (CC\_ID).   
   To enable this, **write a statement that will create a view** called CC\_csr\_view that pulls all columns from the CreditCard table except for the aforementioned fields.  
     
   **Then write the SQL DCL statement** that will grant only SELECT privileges to this view for the Customer Service Rep role.

|  |
| --- |
| **Enter code here**  DROP VIEW CC\_csr\_view;  CREATE VIEW CC\_csr\_view assigned  SELECT  ContentCreator\_id,  exp\_date,  street\_billing,  city\_billing,  state\_billing,  zip\_code\_billing  FROM CreditCard  GRANT SELECT  ON CC\_csr\_view  TO CustomerServiceRep; |