**Name: Ariel Gelman**

**DBMS Security Schema Details**

**DBA Users**

Our database schema can only be seen by database administrators who have the proper clearances and roles assigned through Microsoft Azure. The Centralized Administration will be utilized to arbitrate who will receive specific roles and or entitlements through Active Directory that will either limit or expand individuals depending upon their job functions. Directory roles assigned to individuals will consist of User, Global Administrator, and or a Limited Administrator for which at least several administrative roles can be selected (anything from Helpdesk Admin to a Privileged Role Admin). The individual with the role or job title of Centralized Database Security Administrator (belonging to the proper IT security group) will receive intensive training in database security techniques. With this role will come both the previously mentioned responsibilities and the responsibility of granting capabilities such as SELECT, INSERT, UPDATE, DELETE, or ALL through T-SQL language.

The application front end will be careful and thoroughly inspected for possible SQL Injection attacks. Application front end developers will make sure that input will be read in as string text and that no capability therein exists to use DROP statements that could cause catastrophic damage to the backend database that could be irreparable. Tests will be performed also to ensure that any input received by front end form controls such as text fields do not allow the use of specified characters in the context of semi colons or other specialized characters related to SQL. All the proper guidelines and procedures will be followed for data field sanitization.

Programmers who are working on the frontend application for the BooksRUs CRM will also not be able to view specific rows and or columns for which they are restricted access. This will be done through the creation of database views that are stored procedures.

**CRM Users**

Every individual who has direct contact with or is working in the CRM database will have the priority of making sure they become familiar of the many ways human error can cause problems with data integrity. Strict rules will be created for compliancy to make only certain data visible to the right individuals (again that goes with the programmers as well).

CRM Users will be given a role from a listed of predefined roles that are available within their own database table called **CRM\_Roles**. This will be connected to how and what they can access in the CRM database. Each CRM individual will be able to create a password which is stored within the **CRM\_Password** database table. When a user authenticates with their ID it will go through and match the proper password for their account to then grant then the CRM access to their dashboard. Other credentials are recorded such as the CRM individual’s first and last name along with email address. Associated tasks also will be non-static or can change depending upon when the CRM User updates them. The schema is integral to the way authentication takes place and allows them to seamlessly perform the actions they need to in their BooksRus CRM application.

