1. Privacy Analysis

In our database, the user emails and passwords should only be visible to an administrator, and not to other users. There is not any other private information stored, because all other information should be visible to all users.

1. Security Analysis

Regular users should not be able to add or edit Leaders, because they may compromise the data integrity by entering false data, thus invalidating any reviews and/or ratings. Non-Administrators should not have access to the emails or passwords of other users as stated in the Privacy Analysis, because this would compromise user privacy. Users should only be able to rate any leader once, and accounts would need to have a validated email to prevent users from making multiple accounts to rate a leader multiple times, as this would compromise data integrity and essentially invalidate the entire system.

1. Entity Integrity Analysis
2. Referential Integrity Analysis
3. Business Rule Integrity Analysis

The only business rule integrity that needs to be enforced is leaders. Since they are managed by the administrators, the administrators would have to periodically add leaders to the system and change the status of other leaders as time goes on. Outside of that there is not any other business rule constraints, since that is the only thing the database is being used for.