Security Model Description for Soccer Database

General Overview

- The general overview of the soccer database can be broken down into three components:
    - Account Requirements
    - Users
    - User Actions
- For any user who requires an account for this database there are password requirements and policies set in place to strengthen security and combat where there may be vulnerabilities
    - Passwords must be a minimum of 8 characters in length
    - Passwords must contain one number and one special character (i.e. ! @ # $)
    - Password created may not be the same password within three prior changes
    - Password will automatically expire every 60 days
        - Users will be notified and must change password before expiration
        - If user fails to change password, account will be locked out
- For any user created, it can generally be broken down into three different roles along with different actions. There will be more detailed roles that vary due to access permissions to other team data
    - System admin: account with highest permissions
    - Database editor: may edit tables designated to account
    - Database review: may only view tables in database

Soccer Database in Detail

- User roles for the soccer database follow a hierarchical model
- The system admin will be a specified user(s) who works for the national soccer association. Users with this role can create, delete, and edit all user accounts except for their own account. In addition to this, users in this role also have the same permissions as users in roles below them. Log in credentials are required for this role.
- National Soccer Association will be a specified user(s) who is an employee that reports directly to the national soccer association. Users in this role can view, create, edit, and delete all tables in the database. Log in credentials are required for this role
- Team (system admin of local level) will be a specified user(s) who is an employee that reports directly to a specific team. Users in this role can view, create, edit and delete various tables that correspond to their team. They may view other teams data from a “Fan” role, but does not have edit, create or delete permissions for this data. They may also create, edit, and delete the manager account for the team. Log in credentials are required.
- Manager (head coach of team) will be a specified user(s) who is an employee that reports directly to a specific team. They may view and edit tables with data that corresponds to their team. In addition to this, they may delete athlete or create athlete user accounts with permission of team role. Log in credentials required

- Fan is not necessarily a role in the database. This role represents a person who from a public perspective. Data that is published publicly may be viewed by a fan. People in this role do not have access to the database, but may see the data displayed to them in an output terminal such as a website where the data is published.