Security Plan for Community Assist

Main Actors

The primary actors who will have some interaction with the database are the employees, donors, applicants for grants and the general public. Access to the database will be primarily through the web site. There will also be at least two employees designated as a system administrator.

Use Cases:

The general public should be able to see the services Community Assist offers and the summaries and reports of the charities activities. This will be available without login or registration,

Donors need to register and then login. Once logged in they can donate and see the history and amounts of their own donations, and perhaps schedules and information about special events and rewards. They can also edit some of their own registration information.

Applicants for grants will need to register and login. Once logged in they can apply for a grant and see the history and status of their applications. They can also edit some of their own registration information.

Employees will have a separate login. They will be able to view all tables, register users and edit user information. In addition they can manage applications approving, or disapproving grant application.

The system administrator will have full control over the database and be able to add and edit objects as well as perform system tasks such as back up and restore.

Login and Authentication

There will be two paradigms for login and authentication. Employees will log in directly through a login role with their user name, then they will be assigned to the Employee role. A separate login and user name will be used for the administrative role. The web site will have a separate login for employees only.

Donors and applicants will be logged in through an application role. The application will connect and login with the database. When the user logs in on the web site, their user name and password will be validated against a login table in the database. This process will be mitigated through stored procedures and functions in the database. The userid will be used in Session to limit the viewing of the user to their own materials. All passwords will be hashed.

Roles

Each employee will have a login role. In addition they will be members of the employeerole.
There will be an Admin role with superuser permissions

In addition there will be a ca_application role to which all other registered users will belong by virtue of logging in through the web application.

Schema:

There will be tone other schema besides public: a application schema. Ideally all the user interaction will be through that schema.

It should have views and procedures for

- services offered
- reports and activities
- registering
- applying for a grant
- donating
- viewing one’s own registration information filtered by id
- viewing applications filtered by id
- viewing donations filtered by id

Permissions:

The admin role will have superuser and owner permissions

The Employee role will have CONNECT, USAGE, SELECT, INSERT, UPDATE and EXECUTE on the public schema.

The application role will have CONNECT, USAGE, SELECT, and EXECUTE on the application schema

Individual employee logins will have belong the the Employee role.