Scope

- Initial System
  - SPA web application
- Initial Browser Support
  - Chrome (Latest version)
- Initial Data
  - Geography Data
  - Role Data
  - Permission Data
  - Security Questions Data
  - IP Range Data
- Initial Audience (User Base)
  - All of North America

Security

- Authentication (Medium to Critical)
  - Login
    1. Credentials (username & password) are required to authenticate into the system
    2. Usernames shall be any valid email addresses
    3. Passwords shall have a minimum of 12 characters
    4. Passwords shall have a maximum of 2000 characters
    5. All passwords shall NOT be stored as plaintext
    6. Brute force cracking of passwords will require 50+ years on non-quantum computing systems
    7. Account is disabled (i.e. locked) after 3 invalid login attempts
    8. Only admin accounts can manually re-enable locked accounts
  - Password Reset
    1. Users can update their password during a valid session
    2. Users can only reset their password while not authenticated into the system
    3. Users must provide answers to 3 security questions and a secondary factor when resetting password
  - Logout
    1. Users shall have the ability to manually logout of the system as long as their session is still active
    2. Users shall be automatically kicked off the system after 30 minutes of inactivity
    3. Session inactivity is when the users has not communicated with the server for at least 30 minutes or has visited a new page for at least 30 minutes
    4. User sessions should be automatically extended (sliding session) once a valid activity occurs
- Authorization (Medium to Critical)
  - User Access Control
    1. Users shall not be able to view, execute, or otherwise have access to any functionality, data or content that they should NOT have access to
    2. Users must have a valid session in order for UAC validation to occur
    3. Users should be able to configure fine-grained access to data, functionality and content
    4. Users shall be legal adults to gain access to the system
    5. Users from outside of the User Base scope cannot access the system
    6. Unauthorized users should be informed appropriately
       - UI - error message and redirect to appropriate page
       - Server Request - Error response to client

- Privacy (Medium to High)
  - Terms of Service (End-User License Agreement aka EULA)
    1. Only the system administrators should be able to add, update and delete a EULA
    2. Only one EULA can be active at any given point in time
    3. Users must accept the active active EULA prior to being able to access the system
    4. Users that do not accept the current active EULA cannot use the system
  - User Data Privacy
    1. Users must consent to the collection of any personal identifiable information (PII) and telemetry data
    2. Users can only opt-out of telemetry data collection
    3. Users must be able to view what type of data is being collected about the user by the system
    4. Users can request to delete all collected data at any point in time by deleting account

User Management

- Creation (Medium - High)
  - User Registration
    1. Users must provide username, password, date of birth and location (city, state, country) in order to register
    2. Security questions can also be part of registration process
    3. Users cannot register with a username that already exist within the system (regardless if the account is disabled or not)
  - Admin Registration
    1. Admin accounts can register a user by providing the username, data of birth and location (city, state, country)
    2. Admin accounts cannot create another admin account
    3. The password must be randomly created and given to the user
    4. The security questions and answers must be randomly selected and given to the user
    5. Cannot register with a username that already exist within the system (regardless if the account is disabled or not
    6. On first time login, the user must create a new password and select new security questions & answers
- Activation (Low)
  - Enable User Account
    1. Only admin accounts can activate a disabled normal user account
    2. Active accounts cannot be selected for activation
    3. Admin accounts cannot activate a disabled admin account
    4. Only the system administrator can activate a disabled admin account
  - Disable User Account
    1. Only admin accounts can disable active normal user accounts
    2. Disabled accounts cannot be selected for disabling
    3. When attempting to login, the user will be notified that their account is disabled and access is denied
    4. Admin accounts cannot disable active admin account
    5. Only the system administrator can disable an active admin account
- Deletion (Low)
  - User Delete Account
    1. Users can request to delete their account at any point in time

    2. All PII data related to the account shall be deleted when their account is deleted
  - Admin Delete Account
    1. Admin accounts can delete a normal user account at any point in time
    2. All PII data related to the account shall be deleted when their account is deleted
    3. Admin accounts cannot delete another admin account
    4. Only the system administrator can delete an admin account
- Configuration (Low - High)
  - Admin UAC Configuration
    1. Admin accounts can alter the UAC for normal user accounts
    2. Admin accounts cannot alter the UAC for other admin accounts
    3. Only system administrators can alter UAC of admin accounts
  - Application Specific Configuration
    1. Application Specific

Error Handling

- Client-Side Error Handling (Low - Medium)
  - Exception Handling
    1. All exceptions on the client side will result in a user friendly message when applicable
       - Server request timeouts
       - Invalid Server requests
       - Server error
       - Invalid user input
       - Unauthorized access
       - Contact administrator
    2. Exceptions should not crash the system
    3. Remedy (actionable message) is always provided as part of exception handling
- Server-Side Error Handling (Low - Medium)
  - Exception Handling
    1. All exceptions on the server side will result in a user friendly message if returning to the client
       - Invalid request
       - Server error
       - Unauthorized access
       - Contact administrator
    2. Other than critical faults (server/network shutdown), exceptions should not crash the system

Audit Management

- Logging (Low - Medium)
  - Error Logging
    1. After 100 failed error logs the system administrator should be notified
    2. Only system administrator can delete error logs
    3. All exceptions are logged on the server for all users
       - Date & Time of error
       - Error message
       - Line of Code / Target site
       - Current logged in User
       - User request/action
  - Telemetry
    1. After 100 failed telemetry logs the system administrator should be notified

2. All telemetry data will be logged for all users unless explicit opt out is selected
    - Date and time of user login
    - Date and time of user logout
    - Date and time of user page visit
    - Date and time of user functionality execution
    - Current IP address of logged in user
    - Current Location of logged in user
- Malicious Attacks
    1. All requests to the server will be logged to monitor for denial of service (DOS) attacks

- Log Archiving (Low - Medium)
    - Archiving
        1. All logs older than 30 days are grouped up and backed-up
        2. All logs older than 2 years are grouped up and archived and deleted off of the system
        3. If an archive fails, it should retry after 2 hours
        4. If an archive fails more than 3 times, the archive process stops and the system administrator is be notified

System Analytics

- Usage Analysis Dashboard (Medium - High)
    - Bar Charts
        1. Average successful login per month vs Total registered users showing max and min bars
        2. Average session duration per month showing max and min bars
        3. Failed login attempts vs Successful login attempts
        4. Top 5 average time spent per page of system
        5. Top 5 most used feature in system
    - Line Charts
        1. Timeline of average session duration per month over 6 months
        2. Timeline of number of logged in users per month over 6 month

Data Store Access

- Data Access Layer (Medium - High)
    - Create
        1. Ability to add new records in the data store
        2. If the exact record already exist duplicate entry should not be allowed
        3. If the system does not enough physical space to store new records, then no action takes place on the data store
        4. Operation must be atomic unless explicitly not required by application feature
    - Read
        1. Ability to read a specific subset of data or all data from the data store
        2. If no record is found then no action takes place on the data store
        3. Read limitation depends of data store and machine technical limitations
        4. Operation must be atomic unless explicitly not required by application feature
    - Update
        1. Ability to update existing records stored in the data store
        2. If records cannot be found, then no action takes place on the data store
        3. Operation must be atomic unless explicitly not required by application feature
    - Delete

        1. Ability to delete existing records
        2. If records cannot be found, then no action takes place on the data store
        3. Operation must be atomic unless explicitly not required by application feature
    - Data Restriction
        1. Ability to control the type of data a DAL request has access to retrieve during specific scenarios

Documentation

- User Manual (Low - High)
    - Developer Docs
        1. Access to Developer Docs does not require authentication
        2. The target audience are software developers
    - User Manual
        1. Access to User Manual does not require authentication
        2. User Manual should be an exhaustive resource
        3. Only the system administrator can update the User Manual
        4. The target audience are normal users of the system
    - FAQ
        1. Access to FAQ does not require authentication
        2. FAQ should not be an exhaustive resource
        3. Only the system administrator can update the FAQ
        4. The target audience are normal users of the system