# Security

## Authentication

A mechanism for identifying a valid registered user of Lifelog

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**User Input**

*Required Input*

- Valid security credentials consist of a valid username and valid time-based one-time password (OTP)
- Username
    - The username is the user's email
    - Must be in the [xxxx@xxxx.xxx](mailto:xxxx@xxxx.xxx) format
    - Must not be in used by any other Lifelog account
- OTP is defined in NIST SP 800-63b section 5.1.4.1
    - OTP is changed upon every successful use
    - OTP expires every 2 minutes
    - OTP must be at minimum 8 characters
    - Valid characters will consist of the following:
        - a-z
        - A-Z
        - 0-9

**App Permissions**

- Permission: Write
- Scope: Any unauthenticated user attempting to use the system can attempt to

authenticate

**Target Audience** – Unauthenticated Anonymous Users

**Pre-conditions**
1. Users must not already have an active authenticated session with the system on the current device, otherwise authentication is not possible.
2. Users must be on Login view or attempting to access a protected resource as defined in Authorization

**Success Outcome(s)**
- The system requires the user to authenticate
- The user submits valid security credentials as defined in the User Input section
- The user is automatically navigated to the home view upon successful authentication
- If user is already authenticated, the user should not be able to reach Login view or login functionality
- A timestamp and outcome for each authentication attempt will be recorded

**Failure Outcome(s)**
- The system does not send OTP email. In this case, the system log with context "OTP email send failed"
- The system sends an invalid OTP. In this case, there will be a message saying "Invalid OTP used. Please request a new OTP"
- Upon successful authentication, the user is not automatically navigated to the home view
- Upon successful authentication, the user is automatically navigated to a view that is not the home view
- The user submits the credentials for a disabled account. In this case, there is a message saying "Account is disabled. Perform account recovery first or contact system administrator"

- The user submits invalid credentials. In this case, there should be a message saying "Invalid security credentials provided. Retry again or contact system administrator"

# Authorization

A mechanism for restricting access to protected resources (e.g. functionalities, data, and views) of Lifelog to only valid users

**Effort Points (Hour)** - 50 points

**Complexity Scale**: Medium

**App Permissions**
- Permission: Read
- Scope: Any user attempting to use the system

**Target Audience** - Authenticated Users

**Pre-conditions**
1. User must be authenticated to enforce user-specific restrictions
2. User account must be active (not disabled)

**Success Outcome(s)**
- The operation and timestamp of each unauthorized access will be recorded by the system
- The system must prevent unauthorized users from viewing, modifying or deleting any protected data (scalar or aggregate data)
- The system must prevent unauthorized users from executing any protected functionality
- The system must prevent unauthorized users from viewing or interacting with any protected views

- Any user access modifications should be active upon the next successful authentication by user
- Access is granted when the user attempts to access a protected functionality within authorization scope
- Access is granted to perform read operations when the user attempts to access protected data within authorization scope.
- Access is granted to perform write operations when the user attempts to modify protected data within authorization scope
- Access is granted to the view when the user attempts to access protected views within authorization scope
- System failures from this feature must not result in the system going offline

**Failure Outcome(s)**
- Unauthorized access is not recorded by system when authorization fails. In this case, a system log of failure is attempted.
- User attempts to access a protected functionality outside of authorization scope. In this case, access is denied and a system message is displayed saying "Unauthorized access"
- User attempts to access protected data outside of authorization scope. In this case, access is denied and a system message is displayed saying "Unauthorized access to data"
- User attempts to modify protected data outside of authorization scope. In this case, access is denied and a system message is displayed saying "Unauthorized access to view"
- User attempts to access protected views outside of authorization scope. In this case, access is denied and a system message is displayed saying that this is unauthorized view access
- User attempts to access protected views within authorization scope, but contains protected data that is not within read scope. Access is granted to the view. Upon completion of automatic navigation to view, a system message is displayed saying "Unauthorized access to data", with protected data not visible

within the view.

- User attempts to access protected views within authorization scope, but contains protected data that is not within write scope. Access is granted to the view. Upon completion of automatic navigation to view, protected data is visible within the view. Attempts to modify the data will result in a system message saying "Unauthorized access to data"

# Registration

A mechanism for creating new user accounts within Lifelog

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**User Input**

*Required Input*

- Email
    - Minimum of 3 characters
    - ii. Must be in the format: <valid_characters>@<valid_characters>
    - iii. a-z (case insensitive)
    - iv. 0-9
    - v. May have special characters
        - .
        - -
    - Must not be in used by any other accounts
    - User must confirm email address within 2-hours to complete registration
- Valid date of births begins January 1st, 1970 and ends at current date.
- Zip Code
    - Must be a valid 5 digit zip code within LA County, see Data Source
    - Value is not nullable

**Data Source**

*Origin*

- External

*Type*

- Snapshot

*Details*

- Link:
  https://geohub.lacity.org/datasets/71b2fed2c1f24fc8850f5b7f8d2a320a_26/
- The link contains a downloadable CSV of all zip codes within LA County, this will be stored in the persistent data store

*AuthN*

- None, publicly available data


**App Permissions**

- Permission: Write
- Scope: Lifelog User Account


**Target Audience** - Unauthenticated Anonymous Users


**Pre-conditions**

1. The user must not have an active authenticated session on the application
2. The user is on the Sign Up View


**Success Outcome(s)**

- System administrators cannot be created using Registration view
- All inputs meets validation requirements in the User Input section
- After confirming the email address, a system message is displayed to the user saying "Registration complete for [email address]" within 3 seconds of confirmation completion. The user is automatically navigated to the home view
- User must not have access to Registration View if currently authenticated
- All user accounts must be stored in a persistent data store

**Failure Outcome(s)**

- All inputs do not meets validation requirements in User Input section
- Confirmation email is not sent to the user. In this case, the system attempts to log with context "Confirmation email failure"
- User completes confirmation after 2 hours. In this case, a system message is displayed saying "Confirmation time period has expired. Register again or contact the system administrator."
- User registers with an invalid email. In this case, a system message is displayed saying "Invalid email provided. Retry again or contact system administrator"
- User registers with an invalid date of birth. In this case, a system message is displayed saying "Invalid date of birth provided. Must be within 1/1/1970 to [current date]."
- User completes confirmation within 2 hours, but the system was unable to assign a system-wide username using the user's email. In this case, a system message is displayed saying "Unable to assign username using this email address. Retry again or contact system administrator". Account is not created.
- User completes confirmation within 2 hours, and the system was able to assign a system-wide username using the user's email, but it took longer than 3 seconds. In this case, a system log is saved with the context "Operation exceeded time frame". User Account is created
- The new user account is not saved in the persistent data store

# User Administration

## Account Deletion

A mechanism deleting a user account on Lifelog

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**App Permissions**
- Permission: Delete
- Scope: Any unauthenticated user attempting to use the system can attempt to authenticate

**Target Audience** - All Authenticated User

**Pre-conditions**
1. User must have an active authenticated session
2. User must be on account deletion view
3. User has permission to delete account

**Success Outcome(s)**
- Only an admin account can delete another admin account
- All personal identifiable information (PII) along with the user account data is permanently deleted from the persistent data store. A system message displays "Account deletion successful". Upon acknowledgment of system message, the user is automatically navigated to the home view
- Account deletion is irreversible
- The system must not go offline as the result of failures from this operation

**Failure Outcome(s)**

- The user tries to delete their account and confirms the action, but the system does not delete both PII data or user account data. In this case, "Account deletion failed" is displayed
- Data is not permanently deleted from the system.
- A system message is not shown or the wrong message is shown after all PII data and user account data is permanently deleted from the system
- The user is unable to acknowledge the system message "Account deletion successful" after the successful data deletion.
- The user is not automatically redirected to the home view upon acknowledging the system message

# Usage Analysis Dashboard

A visualization mechanism for gaining insight on user behavior within Lifelog

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**App Permissions**
- Permission: View
- Scope: Admin and Root Admin User

**Target Audience** - All Authenticated User

**Pre-conditions**
1. Persistent data store must be active
2. Persistent data store must be accessible by the system
3. User must have an active authenticated session on the current device
4. User must be on the Usage Analysis Dashboard View
5. User must be a system administrator

**Success Outcome(s)**
- Only Admin and Root Admin user can access the dashboard
- All data successfully fetched from the persistent data store
- The following Key Performance Indicators (KPIs) are displayed
  - The number of success and failed login attempts per month over selected time span (trend chart)
  - The number of success and failed registrations per month over selected time span (trend chart)
  - Top 3 longest page visits in seconds
  - Top 3 most used feature
  - Two application specific feature metric
- The KPIs can be displayed with the following time spans

- 6 months
- 12 months
- 24 months
- All KPI data must be automatically refreshed in intervals of 60 seconds
- The view must load within 15 seconds upon completion of navigation.
- System failures from this feature must not result in the system going offline

**Failure Outcome(s)**
- An Admin or Root Admin user is unable to access the dashboard
- The view does not load within 15 seconds upon accessing the dashboard
- All KPI data are not refreshed every 60 seconds
- KPI data refresh takes longer than 60 seconds

# Lifelog Item (LLI) Management

## LLI1 User Story[17]: Create LLI[3]

As an authenticated user, I can create one LLI[3] at a time to track my life change progress.

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**User Input**

*Required Input*

- Title of LLI[3]
    - Must only contains  alphanumeric values between 1-50 characters long
    - The value is not nullable
- Category/Categories of LLI[3]
    - The valid options are "Mental Health[5]", "Mental Health[5]", "Physical Health[6]", "Outdoor[7]", "Sport[8]", "Art[9]", "Hobby[10]", "Thrill[11]", "Travel[12]", "Volunteering[13]", and "Food[14]"
    - The option is not nullable

*Optional Input*

- Description of LLI[3]
    - Must consist only of alphanumeric values between 0-200 characters long
    - Default to null
- Status of LLI[3]
    - The valid options are "Active", "Completed", "Postponed"
    - The option is not nullable
    - Default to "Active"

- Visibility of LLI[3]
  - The valid options are "Public, Private"
  - The option is not nullable
  - Default to "Public"
- Deadline of LLI[3]
  - Must be a valid date in the format MM/DD/YYYY
  - The date must be between 01/01/1900 and 12/31/2100
  - Default to null
- Cost of LLI[3]
  - Must be a numerical value greater or equal to $0 USD
  - The unit of the cost is USD
  - Cost cannot be non-integers
  - Cost cannot exceed $1 million USD
  - Default to null

**App Permissions -**
- Permission: Write
- Scope: LLI[3]

**Target Audience -** All authenticated Normal User

**Pre-conditions**
1. The user is registered
2. The user is authenticated
3. The authenticated user is in the LLI[3] Management view

**Success Outcomes**
- All inputs meets validation requirements in User Input section
- The new LLI[3] is saved to the persistent data store
- The new LLI[3] is added to the authenticated user's account in the relational database

- "LLI successfully created" is displayed to the user, if the LLI[3] has been created in the persistent data store
- A LLI[3] template containing the new LLI[3] information is shown in the LLI[3] Management View within 3 seconds of the creation confirmation
- The LLI[3] creation is logged in the persistent data store
- The log includes the following:
  - Timestamp
    - When the LLI creation form is submitted
    - When the LLI creation form is saved in the persistent datastore
    - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
    - Timestamp is recorded relative to PST
  - Log level (Success)
  - Log type (Create)
  - Log Message: "LLI successfully created"

**Failure Outcomes**
- All inputs do not meet validation requirements in the User Input section. In this case, "LLI inputs are invalid, please try again" is displayed to the user
- The new LLI[3] is not saved to the relational database. In this case, "LLI fails to saved" is displayed to the user
- The new LLI[3] is not added to the authenticated user's account in the relational database. In this case, "LLI fails to saved to user's account" is displayed to the user
- A LLI[3] template containing the new LLI[3] information is not shown in the LLI[3] Management View within 3 seconds of the creation confirmation. In this case, "Operation exceeded time frame" is displayed
- The LLI[3] creation is not logged in the persistent data store
- The operation is logged, but the log does not accurately depict any of the following:
  - Timestamp
    - When the LLI creation form is submitted

- When the failure occurs in the deletion process
- Timestamp will be in YYYY-MM-DD-hh-mm-ss format
- Timestamp is recorded relative to PST
  - Log level (Error)
  - Log type (Create)
  - Log message: "LLI creation encountered an error...", along with information identifying the error

# LLI2 User Story[17]: Delete LLI[3]

As an authenticated user, I can delete one LLI[3] at a time to remove a prospective life change, to stay focused on my personally attainable LLI[3]

**Effort Points (Hour)** - 100 points

**Complexity Scale**: Medium

**App Permissions**
- Permission: Delete
- Scope: LLI[3]

**Target Audience** - All authenticated Normal User

**Pre-conditions**
1. The user is registered
2. The user is authenticated
3. The authenticated user is in the LLI[3] Management view

**Success Outcome(s)**
- The LLI[3] is removed from the persistent data store
- The LLI[3] is removed from the authenticated user's account in the persistent data store

- The LLI[3] template containing the LLI[3] information is no longer shown in the LLI[3] Management View within 3 seconds of the user initializing the delete action
- "The LLI is successfully deleted" is displayed to the user, if the LLI[3] has been deleted
- The delete operation is logged in the persistent data store
- The log includes the following:
    - Timestamp
        - When the LLI deletion form is submitted
        - When the LLI is deleted from the persistent data store
        - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
        - Timestamp is recorded relative to PST
    - Log level (Success)
    - Log type (Delete)
    - Log Message: "LLI successfully deleted"

**Failure Outcome(s)**
- The LLI[3] is not removed from the persistent data store. In this case, "The LLI is not successfully deleted" is displayed to the user
- The LLI[3] is not removed from the authenticated user's account in the persistent data store. In this case, "The LLI is not successfully deleted from the user's account" is displayed to the user
- The LLI[3] template containing the LLI[3] information is still shown in the LLI[3] Management View within 3 seconds of the user initializing the delete action. In this case, "Operation exceeded time frame" is displayed
- The delete operation is not logged in the persistent data store
- The operation is logged, but the log does not accurately depict any of the following:
    - Timestamp
        - When the LLI deletion form is submitted
        - When the failure occur in the deletion process

- Timestamp will be in YYYY-MM-DD-hh-mm-ss format
- Timestamp is recorded relative to PST
  - Log level (Failure)
  - Log type (Delete)
  - Log message: "LLI deletion encountered an error...", along with information identifying the error

# LLI3 User Story[17]: Edit LLI[3]

As an authenticated user, I can edit one LLI[3] at a time to manage my life change details, ensuring my goal setting is accurate.

**Effort Points (Hour)** - 50

**Complexity Scale**: Medium

**User Input**

*Optional Input*

- LLI[3] title
  - Must only contain alphanumeric values
  - Must be between 1-50 characters long
  - The value is not nullable
  - Default value is current title
- Category/Categories of LLI[3]
  - The valid options are "Mental Health[5]", "Physical Health[6]", "Outdoor[7]", "Sport[8]", "Art[9]", "Hobby[10]", "Thrill[11]", "Travel[12]", "Volunteering[13]", and "Food[14]"
  - The option is not nullable
  - Default value is the current category/categories
- Description of LLI[3]
  - Must consist only of alphanumeric values between 0-200 characters

long

- ○ The value is nullable
- ○ Default value is the current description

- Status of LLI[3]
  - ○ The valid options are "Active", "Completed", "Postponed"
  - ○ The option is not nullable
  - ○ Default value is the current status
- Visibility of LLI[3]
  - ○ The valid options are "Public, Private"
  - ○ The option is not nullable
  - ○ Default value is the current visibility
- Deadline of LLI[3]
  - ○ Must be a valid date in the format MM/DD/YYYY
  - ○ The date must be between 01/01/1900 and 12/31/2100
  - ○ The option is nullable
  - ○ Default value is the current deadline
- Cost of LLI[3]
  - ○ Must be a numerical value greater or equal to $0 USD
  - ○ The unit of the cost is USD
  - ○ Cost cannot be non-integers
  - ○ Cost cannot exceed $1 million USD
  - ○ Default cost is the current cost

**App Permissions**
- Permission: Write
- Scope: LLI[3]

**Target Audience** - All authenticated Normal User
**Pre-conditions**
1. The user is registered
2. The user is authenticated

3. The authenticated user is in the LLI[3] Management view

**Success Outcome(s)**
- All inputs meets validation requirements in User Input section
- Changes to the LLI[3] attributes are reflected in the persistent data store accurately
- "LLI successfully updated" is displayed to the user, if the LLI details are changed
- The LLI[3] view containing the LLI[3] information reflects the changes within 3 seconds of the user initializing the change action, if the changes to the LLI attributes are successful
- The edit operation is logged in the persistent data store
- The log includes the following:
  - Timestamp
    - When the LLI edit form is submitted
    - When the changes to the LLI are saved to the persistent data store
    - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
    - Timestamp is recorded relative to PST
  - Log level (Success)
  - Log type (Edit)
  - Log Message: "LLI successfully edited"

**Failure Outcome(s)**
- All inputs do not meet validation requirements in the User Input section. In this case, "LLI inputs are invalid, please try again" is displayed to the user
- Changes to the LLI[3] attributes are not reflected in the persistent data store accurately. In this case, "LLI updates failed" is displayed to the user. The LLI instance in the data store should not be changed.
- The LLI[3] view containing the LLI[3] information does not reflect the changes within 3 seconds of the user initializing the change action, if the changes to the LLI attributes are successful. In this case, "Operation exceeded time frame" is

displayed.

- The edit operation is not logged in the persistent data store
- The operation is logged, but the log does not accurately depict any of the following:
    - Timestamp
        - When the LLI edit form is submitted
        - When the failure occur in the LLI edit process
        - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
        - Timestamp is recorded relative to PST
    - Log level (Failure)
    - Log type (Edit)
    - Log message: "LLI edit encountered an error…", along with information identifying the error

# User Form

## LLU1 User Story[17]: Create User Form[16]

As an authenticated user, upon my first sign-in, I can rank the 10 categories of LLI[3] in order of preference to personalize my recommendation engine's recommendations.

**Effort Points (Hour)** - 50 points

**Complexity Scale**: Medium

**User Input**

*Required Input*
- Rankings of the following categories in relation to each other:
  - The categories to be ranked are "Mental Health[5]", "Physical Health[6]", "Outdoor[7]", "Sport[8]", "Art[9]", "Hobby[10]", "Thrill[11]", "Travel[12]", "Volunteering[13]", and "Food[14]"
- Each category must have a unique ranking
- The rank for a category must be a numerical value between 1-10
- The ranking for a category is not nullable

**App Permissions**
- Permission: Read and Write
- Scope: Lifelog User Account

**Target Audience** - Authenticated Normal User logging in for the first time

**Pre-conditions**
1. The user is registered
2. The user is authenticated
3. The authenticated user is signed in for the first time

**Success Outcome(s)**

- All inputs meets validation requirements in User Input section
- The user rankings are saved in the persistent data store
- The user rankings are added to the user's account in the persistent data store
- "User rankings successfully saved" is displayed to the user, if the rankings are successfully saved
- The user rankings are saved to the persistent data store within 3 seconds of the form submission
- The create operation of the user form is saved to the persistent datastore
- The log includes the following:
    - Timestamp
        - When the LLI user form is submitted
        - When the LLI user form is saved to the data store
        - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
        - Timestamp is recorded relative to PST
    - Log level (Success)
    - Log type (Create)
    - Log Message: "User Form successfully created"

**Failure Outcome(s)**

- All inputs do not meet validation requirements in the User Input section. In this case, "Invalid input, please try again" is displayed to the user
- The user rankings are not saved in the persistent data store. In this case, a message is displayed saying "User Form failed to save, please try again later or contact system administrator"
- The user rankings are not added to the user's account in the persistent data store. In this case, a message is displayed saying "User Form failed to save, please try again later or contact system administrator"
- The user rankings are not saved to the persistent data store within 3 seconds of the form submission. In this case, "Operation exceeded time frame" is displayed to the user

- A log of the completion of the user rankings is not saved in the persistent data store
- The operation is logged, but the log does not accurately depict any of the following:
  - Timestamp
    - When the LLI user form is submitted
    - When the failure occur in the user form creation process
    - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
    - Timestamp is recorded relative to PST
  - Log level (Failure)
  - Log type (Create)
  - Log message: "User Form creation encountered an error…", along with information identifying the error

# LLU2 User Story[17]: Edit User Form[16]

As an authenticated user, I can edit my rankings of the 10 categories of LLI in my User Form to tailor the application recommendation to my need

**Effort Points (Hour)** – 50 points

**Complexity Scale**: Medium

**User Input**

*Optional Input*

- Rankings of the following categories in relation to each other:
  - The categories to be ranked are "Mental Health[5]", "Physical Health[6]", "Outdoor[7]", "Sport[8]", "Art[9]", "Hobby[10]", "Thrill[11]", "Travel[12]", "Volunteering[13]", and "Food[14]"
- Each category must have a unique ranking
- The rank for a category must be a numerical value between 1-10
- The default value for a rank of a LLI is the current rank of that LLI
- The ranking for a category is not nullable

**App Permissions**

- Permission: Read and Write
- Scope: Lifelog User Account

**Target Audience** – All authenticated Normal User

**Pre-conditions**

1. The user is registered
2. The user is authenticated
3. The authenticated user is in the User Profile view

**Success Outcome(s)**

- All inputs meets validation requirements in User Input section
- Changes to the User Form, if any, are saved in the persistent data store
- "User Form successfully saved" is displayed to the user if the User Form is successfully updated
- Changes to the User Form, if any, are saved in the data store within 3 seconds
- The operation is logged in the data store
- The log includes the following:
  - Timestamp
    - When the LLI user form changes are submitted
    - When the LLI user form changes are saved to the data store
    - Timestamp will be in YYYY-MM-DD-hh-mm-ss format
    - Timestamp is recorded relative to PST
  - Log level (Success)
  - Log type (Edit)
  - Log Message: "User Form successfully edited"

**Failure Outcome(s)**
- All inputs do not meet validation requirements in the User Input section. In this case, a message is displayed saying "Invalid input, please try again"
- Changes to the User Form, if any, are not saved in the relational database. In this case, a message is displayed saying "User Form failed to save. Please try again"
- Changes to the User Form, if any, are not saved in the data store within 3 seconds. In this case, "Operation exceeded time frame" is displayed to the user
- The operation is not logged in the persistent data store
- The operation is logged, but the log does not accurately depict any of the following:
  - Timestamp
    - When the LLI user form changes are submitted
    - When the LLI user form changes are saved to the data store
    - Timestamp will be in YYYY-MM-DD-hh-mm-ss format

- - - Timestamp is recorded relative to PST
  - Log level (Failure)
  - Log type (Edit)
  - Log message: "User Form edit encountered an error…", along with information identifying the error