

Musi-Cali

Business Requirements Document

11/26/23

Product Name: Musi-Cali

Team Name: Team Phoenix

Team Members:

Julie Reyes (Team Leader)

Jason Jitsiripol

Shane Kerr

Diego Garcia

Kihambo Muhumuza

Project Github: [GitHub - JPJ-5/TeamPhoenix](#)

Table of Contents

Version History.....	4
Product Wide Scope.....	5
Distinct User Types.....	5
User Roles.....	6
App Permissions Matrix.....	7-8
 Default Behaviors.....	 8-12
Operation Time Limit.....	8-9
Asynchronous Processing.....	9
No Records in Data Store.....	9-10
Data Store Offline.....	10
Unauthorized Access to a Protected Resource.....	10-11
Viewing.....	11
Input Validation.....	11
Operational Logging.....	12
 System Requirements.....	 12-50
Authentication.....	12-16
Authorization.....	16-19
Logout.....	19-21
User Administration.....	21-32
User Management.....	32-42
Usage Analysis Dashboard.....	42-48
User Privacy Control.....	48-50
 Phase 1 Feature Requirements.....	 50-90
Artist Portfolio.....	50-58
Artist Profile Calendar.....	58-66
Collaboration Search.....	66-70
Collab Feature.....	70-77
Bingo Board.....	77-84
Tempo Tool.....	84-88
Scale Display.....	88-90
 Glossary.....	 91

Version History

Version	Date	Authors	Changes
1.0	10/11/2023	Team	Document Initialization
1.1		Aiden	Refactored UM to UA and then added a new UM section. Finished UM and now revising UA and CS.
1.2	11/12/23	Nathan, Kihambo, Jacob, Aiden	Added Core Requirements and updated table of contents
1.3	11/22/23	Team	Applied app permission matrix, user roles, default behaviors, logging, error handling, and reformatting.
1.4	11/26/23	Team	Revised the following Asynchronous Processing, No Records in Data Store, Data Store Offline, unauthorized access to a protected resource, Input Validation, Authentication & Logout, UA-registration, UM- account deletion
1.5	3/16/2024	Joshua	Removed unleaded features from existing team. Updated the index and fixed some formatting errors.

Introduction

Product- Wide Scope:

Musi-Cali is designed as a streamlined approach that will help musicians collaborate together and/or find work locally.

- Will be deployed as a single page web application.
- Unregistered users must be 14 and older to make an account.
- Will be supported by Chrome Desktop version 105.0.5195.127 and later in 1920 x 1080 pixel resolution.
- Supports mobile version and mobile display.
- Will cover the city of Long Beach (PST Time Zone) in US English, and eventually cover the rest of Southern California in the future (PST, CST, EST).
- Will operate utilizing a 12 hour clock, gregorian calendar, and imperial system.

Distinct User Types:

Unregistered User (Prospective User):

- An unregistered user in Musi-Cali is someone who has initiated the registration process but has not yet completed it. They may have provided some initial information but have not verified their email address or finalized the registration.
- Can start the process of creating a Musi-Cali account but cannot access features until authenticated and registered.
- Permissions:
 - Initiating the Musi-Cali account creation process.
 - Providing the required registration information (email, password, name).
 - Receiving a confirmation email for account verification.
 - Limited access to Musi-Cali until the registration is finalized.

Registered User (Captured User):

- A registered user in Musi-Cali is someone who has successfully created an account and can log in using their credentials.
- Can access registered-user-specific features, customize their profile, and interact with the platform as an authenticated user.

Authenticated User (Active User):

- An authenticated user in Musi-Cali is a subset of registered users who have logged into their accounts and are actively using the platform's features.
- Can fully utilize all features available to registered users after authenticating themselves by logging in.

User Roles:

Feature	Talent Role	Admin Role
Logout		
Authentication		
Authorization		
Registration		
Account Recovery		
Account Deletion		
User Privacy Control		
User Management		
Usage Analysis Dashboard		
Collaboration Search		
Artist Portfolio		
Tempo Tool		
Artist Profile Calendar		
Scale Display		
Bingo Board		
Collab Feature		

App Permissions Matrix:

Feature	Read	Create	Write	Delete
Logout			Edit Authentication Status	
Authentication	Verify Login Credentials		Edit Authentication Status	
Authorization	Verify			

	Permission to use Resource			
Registration	Verify Unique Username	Creates Account		
Account Recovery	Verify Login Credentials	Create Account Recovery Request		
Account Deletion	Verify Login Credentials			Delete Account
User Privacy Control			Edit Privacy Status	
User Management	Read Users	Create Account	Edit Account	Delete Account
Usage Analysis Dashboard	Read User Metric			
Collaboration Search	Read User Data			
Artist Portfolio	Read Portfolio File	Create Portfolio File	Edit Portfolio File	Delete Portfolio File
Tempo Tool	Read Beats Per Minute		Edit Beats Per Minute	
Artist Profile Calendar	Read Calendar Data		Edit Calendar Data	Delete Calendar Data
Scale Display	Read Scale			
Bingo Board	Read Post Data	Create New Post	Edit Post	Delete Post
Collab Feature	Read Collab	Create New Collab	Edit Collab	Delete Collab

Default Behaviors

Default behaviors will work as follows unless explicitly redefined in a functionalities user story.

Operation Time Limits

Measure of operation timeliness:

1. Operation length of 0.1 seconds - 3.0 seconds:
 - a. If the response time falls within this range, it is a successful outcome.
 - i. Logging info:
 1. Datetime
 2. Log Level: Info
 3. Log Category: Business
 4. Description:
 - a. Feature
 - b. User Story ID
 - c. Log Message: “[operation] took less than 3 seconds.”
2. Operation length of 3.1 seconds - 5.0 seconds:
 - a. If the response time falls within this range, it is a successful outcome but not ideal for the system.
 - i. System will display a message to the user saying: “[operation] took longer than expected.”
 - ii. Logging info:
 1. Datetime
 2. Username (if registered otherwise NULL)
 3. Log Level: Warning
 4. Log Category: Business
 5. Description:
 - a. Feature
 - b. User Story ID
 - c. Log Message: “[operation] took longer than 3 seconds and less than 5 seconds.”

3. Operation length 5.1 seconds or longer:
 - a. If the response time falls within this range, it is regarded as an unacceptable failure outcome and an error is logged.
 - i. System will display a message to the user saying “[Operation] timed out.”
 - ii. Logging info:
 1. Datetime
 2. Username (if registered otherwise NULL)
 3. Log Level: Error
 4. Category: Business
 5. Description:
 - a. Feature
 - b. User Story ID
 - c. Error Message: “Timed out after [operation] took longer than 5 seconds.”

Asynchronous Processing

- Each step in a user story will perform synchronously but each user story will perform asynchronously from one another.
- Logging operations will perform asynchronously.
- Functionalities will not impede the user from interacting with the system.

No Records in Data Store

1. If no records are found in the persistent data store and the lack of data does not impede feature operational functionality the system will display a message to the user saying: “No records for [requested data] could be found.”
 - a. Allows them to continue using functionality.
 - b. Logging info:
 - i. DateTime in UTC format
 - ii. Username (if registered otherwise NULL)
 - iii. Log Level: Warning
 - iv. Log Category: Data Store
 - v. Description:
 1. Feature: Feature attempting to access data store
 2. User Story ID
 3. Log Message: “[Feature] requested to access [requested data] and found no records.”

2. If no records are found in the persistent data store and the functionality requires that data to continue the system will display a message to the user saying: “No records for [required data] could be found, cannot use [feature] right now.”
 - a. Authenticated user is returned to home view.
 - b. Logging info:
 - i. DateTime in UTC format
 - ii. Username (if registered otherwise NULL))
 - iii. Log Level: Error
 - iv. Log Category: Data Store
 - v. Description:
 1. Feature: Feature attempting to access data store
 2. User Story ID
 3. Log Message: “[Feature] required access to [required data], but found no records.”

Data Store Offline

1. The system will display a message to the user saying: “The [operation] was unable to be completed because the data store is offline.”
 - a. The operation failure is not logged due to the offline data store.

Unauthorized Access to a Protected Resource

1. When a protected resource is attempted to be accessed outside of a user’s scope of authorization a warning is logged:
 - a. Logging info:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Data
 - v. Description:
 1. Feature
 2. User Story ID
 3. Log Message: “Unauthorized access of [Feature]’s protected resource on User Story ID: [User Story ID].”
 - b. If the protected resource has a UI component, then the system displays an error message, “UI Component on [Feature]’s protected resource is unavailable.”

Viewing

1. Successful view of feature:
 - a. The feature's display successfully loads for the user to view completely
 - i. Logging info:
 1. DateTime in UTC format
 2. Username (if registered otherwise NULL)
 3. Log Level: Info
 4. Log Category: View
 5. Description:
 - a. Feature
 - b. User Story ID
 - c. Log Message: "Successful view of [feature][User Story ID]."
2. Unsuccessful view of feature:
 - a. The feature's display fails to load for the user to view completely
 - i. System will display a message to the user saying "[Feature] has failed to display."
 - ii. Logging info:
 1. DateTime in UTC format
 2. Username (if registered otherwise NULL)
 3. Log Level: Error
 4. Log Category: View
 5. Description:
 - a. Feature
 - b. User Story ID
 - c. Error Message: "Unsuccessful display of [Feature][User Story ID]."

Input Validation

1. During occasions where a user inputs an incorrect input the system does not recognize, the system will respond via displaying a message saying "User entered invalid input. Please try again."
 - a. Logging info:
 - i. DateTime in UTC format
 - ii. Username (if registered otherwise NULL)
 - iii. Log Level: Error
 - iv. Log Category: Data
 - v. Description:

1. Feature
2. User Story ID
3. Error Message: “Invalid input of [Feature][User Story ID].”

Operational Logging

Anytime an operation takes place, it will be logged in the following format:

1. Date time in Coordinated Universal Time (UTC) format:

YYYY-MM-DD HH-MM-SS (YEAR-MONTH-DAY HOURS-MINUTES-SECONDS)
2. Username (if registered otherwise NULL)
3. Log Level:
 - a. Info - for tracking the flow of system
 - b. Debug - for tracking key information crucial to maintainers of the system
 - c. Warning - for tracking events that may lead to system failures
 - d. Error - for tracking system errors
4. Category:
 - a. View
 - b. Business
 - c. Server
 - d. Data
 - e. Data Store
5. Description (Dependent on Failure or Success):
 - a. “[Feature] - [User Story ID] : [Error/Log Message]”
 - i. Error/Log message is dependent on failure or success outcome

System Requirements

Note:

- All effort points are in units of hours. For example, 7 Effort Points = 7 Hours.

Authentication

A method of securely logging into user registered accounts using a one time password sent to their emails.

A - 1: As a registered and unauthenticated user, I want to identify and authenticate myself as a valid registered user of Musi-Cali.

Complexity Level:

- High
- Effort points: 16

App Permissions:

- Permission: Write
- Scope: Authentication status

Target Audience:

- Anyone who is a registered user of Musi-Cali

Required Inputs:

1. The unauthenticated user must provide valid security credentials whenever attempting to authenticate with the system
 - a. Username
 - i. Minimum 8 characters
 - ii. Maximum 30 characters
 - iii. Must not be occupied by an already-existing user
 - iv. Must not be nullable
 - v. Valid characters will consist of the following:
 1. a-z
 2. A-Z
 3. 0-9
 4. Special characters:
 - a. .
 - b. -
 - c. @
 - b. OTP (One-Time Password) as defined in NIST SP 800-63b section 5.1.4.1. It will be sent through to the registered account's email.
 - i. OTP expires every 2 minutes
 - ii. Valid characters will consist of the following:
 1. a-z
 2. A-Z
 3. 0-9

Pre-conditions:

1. The user must not already have an active authenticated session on the current device, or else authentication is not possible
2. The user must be on login view or attempting to view a protected resource as defined in authorization

Success Outcomes:

1. The system requires the unauthenticated user to authenticate.
2. The unauthenticated user presents valid security credentials.
3. The now authenticated user is automatically navigated to the user's home page upon successful authentication.
4. If the user is already authenticated, the user should not be able to view the login view.
5. The OTP expires after 3 minutes after being sent to the user.
6. Each authentication attempt is logged in the data store which includes:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Business
 - e. Description:
 - i. Feature: Authentication
 - ii. User Story ID: A - 1
 - iii. Log Message: "Authentication successful"

Failure Outcomes:

1. The system fails to send OTP email:
 - a. If this happens, the system will print out: "OTP email failed to send, try again."
 - b. Error is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Description
 1. Feature: Authentication
 2. User Story ID: A - 1
 3. Error Message: "OTP email failed to send"
2. The system sends OTP email with an invalid OTP:
 - a. If this happens, the system will print out: "OTP was invalid. Please request a new OTP to be sent."
 - b. Error is logged:
 - i. DateTime in UTC format

- ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Description
 - 1. Feature: Authentication
 - 2. User Story ID: A - 1
 - 3. Error Message: "Invalid OTP sent"
- 3. The user submits valid security credentials for the enabled account. Automatic navigation does not take place.
 - a. Error is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: View
 - v. Description
 - 1. Feature: Authentication
 - 2. User Story ID: A - 1
 - 3. Error Message: "Automatic navigation to home view failed"
- 4. User submits valid security credentials for the enabled account. User is directed somewhere other than the home view after being successfully authenticated.
 - a. Error is logged:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: View
 - v. Description
 - 1. Feature: Authentication
 - 2. User Story ID: A - 1
 - 3. Error Message: "Failed to navigate to user's home view"
- 5. User submits valid security credentials for a disabled account.
 - a. If this happens, the system will print a message saying: "Account is disabled. Perform account recovery first or contact system administrator."
 - b. Info is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 - 1. Feature: Authentication
 - 2. User Story ID: A - 1

3. Info Message: “User authenticated a disabled account.”
6. User submits invalid username or invalid OTP.
 - a. If this happens, the system will print a message saying: “Invalid security credentials provided. Retry or contact system administrator”
 - b. Info is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 1. Feature: Authentication
 2. User Story ID: A - 1
 3. Info Message: “Invalid security credentials”
7. The system fails to log authentication attempt.
 - a. Warning is logged:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Description
 1. Feature: Authentication
 2. User Story ID: A - 1
 3. Warning Message: “Failed to log authentication attempt.”
8. Authentication takes longer than 3 seconds
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Authentication
 - ii. Feature ID: A - 1

Authorization

A layer of security that validates specific user-role app permissions.

A - 1: As an authenticated user, I want to access protected resources in Musi-Cali so I can navigate the app according to my account permissions.

Complexity Level:

- High

- Effort points: 16

App Permissions:

- Permission: Read
- Scope: Verify authenticated user permissions

Target Audience:

- Any authenticated user attempting to use Musi-Cali's functionalities.

Required Inputs:

1. The timestamp and outcome for each unauthorized access will be logged by the system in DateTime UTC format.
2. The system must prevent unauthorized users from executing any protected functionality.
3. The system must protect views from unauthorized users.
4. System failures from this feature must not result in the system going offline.
5. Authorization must take less than 3 seconds upon invocation.

Pre-conditions:

1. Unauthenticated users will only be able to access the login view.
2. The user must be authenticated to enforce user-specific restrictions.
3. The users account must be active.
4. Unauthorized users are unable to view, modify, delete any protected (scalar or aggregate data).
5. Any user access permission modifications should be active upon the next successful authentication by user.

Success Outcomes:

1. The authenticated user attempts to access a protected functionality within authorization scope. Access is granted to use functionality.
2. The authenticated user attempts to access protected data within authorization scope. Access is granted to perform read operations.
3. The authenticated user attempts to modify protected data within authorization scope. Access is granted to perform write operations.
4. The authenticated user attempts to access protected views within authorization scope. Access is granted to the view. Authorized user is automatically navigated to view.

Failure Outcomes:

1. Unauthorized access is not recorded by the system when authorization fails. A system log of failure is attempted
 - a. Log will be recorded according to "Unauthorized Access of a Protected Resource"

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 2. User attempts to access a protected functionality outside of authorization scope. Access is denied and a system message displays “Unauthorized access”.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 3. User attempts to access protected data outside of authorization scope. Access is denied and a system message displays “Unauthorized access to data”.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 4. User attempts to modify protected data outside of authorization scope. Access is denied and a system message displays “Unauthorized access to data”.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 5. User attempts to access protected views outside of authorization scope. Access is denied and a system message displays “Unauthorized access to view”.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 6. 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 displays “Unauthorized access to data” with protected data not visible within the view.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
- 7. 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 that displays “Unauthorized access to data”.
 - a. Log will be recorded according to “Unauthorized Access of a Protected Resource”

Default behavior

- i. Feature: Feature being accessed
 - ii. User Story ID: Feature functionality being accessed
8. Authorization and system messaging takes longer than 3 seconds to take place.
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Authorization
 - ii. Feature ID: A - 1

Logout

Users have the ability to logout and deauthenticate their registered accounts from an active authenticated session.

L - 1: As an authenticated user, I want to logout and end my active session of Musi-Cali.

Complexity Level:

- Medium.
- Effort points: 10

App Permissions:

- Permission:
 - Write
- Scope:
 - Editing authentication status

Target Audience:

- Authenticated talent and Admin role users that want to deauthenticate their account.

Pre-conditions:

1. User must have an active authenticated session.
2. User must be on logout view.

Success Outcomes:

1. When the user chooses the logout option, within 3 seconds, the authenticated session is deauthenticated.
 - a. A system message displays: “Logout successful!”
 - b. Within 3 seconds after closing the display message the user is returned to the home view with default culture settings.
2. If the user is not authenticated then the system will not logout.

3. Each logout attempt is logged in the data store which includes:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Business
 - e. Description:
 - i. Feature: Logout
 - ii. User Story ID: L - 1
 - iii. Log Message: "Logout successful"

Failure Outcomes:

1. User performs logout request. The active session has ended. The user is not automatically navigated to the default home view. A system message displays "Logout operation error".
 - a. Logging format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: View
 - v. Description
 1. Feature: Logout
 2. User Story ID: L - 1
 3. Error Message: "Failed to navigate to default home view after logout"
2. User performs logout request. The active session has ended. The user is automatically navigated to the default home view, but not set to the default culture settings. A system message displays "Logout operation error".
 - a. Logging format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Server
 - v. Description
 1. Feature: Logout
 2. User Story ID: L - 1
 3. Error Message: "Culture settings failed to update to default settings"
3. The logout process takes longer than 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: Logout
 - ii. Feature ID: L - 1

User Administration:

Users have the ability to create, delete, or request recovery for their accounts. All users have access to these functionalities.

UA-1: As an unregistered user, I want to create a Musi-Cali account to access registered-user content.

Complexity Level:

- Medium
- Effort Points: 9

App Permissions:

1. Permission:
 - a. Read
 - b. Create
2. Scope:
 - a. Check for a unique email and username
 - b. Create registered account

Target Audience:

- Any unregistered user who wants to create a new registered, non-administrative, account on Musi-Cali.

Required Inputs:

1. Unique username (5-30 characters consisting of):
 - i. Must not be occupied by an already-existing user
 - ii. Must not be nullable
 - iii. Valid characters will consist of the following:
 1. Case insensitive letters: a-z
 2. 0-9
 3. Special characters:
 - a. .
 - b. -
 - c. @
2. Unregistered user email (3-254 Characters consisting of):
 - a. Cannot already exist in the data store.

- b. Format: <valid_characters>@<valid_characters>.<valid_characters>
 - i. Case insensitive letters: a-z
 - ii. Numbers: 0-9
 - iii. Symbols:
 - 1. .
 - 2. _
 - iv. The email address must comply with RFC 822 standards.
 - v. The local part of the email (before the '@') and the domain part (after the '@') should consist of valid characters as specified above.
 - vi. The domain part must include at least one period (.) with valid characters on both sides.
- 3. First Name (2-25 Characters consisting of):
 - a. Case insensitive letters: a-z
- 4. DOB (Valid dates include from 01/01/1970 to Present).
- 5. Email confirmation
 - a. Unregistered user will be sent an email confirmation link that they must confirm within 2-hours to complete account registration.

Optional Inputs:

- Last Name
 - Defaults to null.
 - 2-25 Characters consisting of:
 - Case insensitive letters: a-z
- Artist Occupation:
 - Defaults to null.
 - The user selects one of the following options for their artist portfolio:
 - Composer
 - Arranger
 - Producer
 - Instrumentalist

Pre-Conditions:

1. Users must not have an existing active authenticated session.
2. Unregistered users are connected to, able to see, and have access to the registration page.
3. System administrators cannot be created using this registration functionality.
4. Failures from this feature do not result in the system going offline.

Success Outcomes:

1. Confirmation of account registration is sent to the email registered on the new account.
2. User confirms registration confirmation link inside their email within 2 hours after

- confirmation link is sent to their email.
3. The newly registered account is saved to the persistent data store.
 4. Within 3 seconds of confirmation of the email the system needs to display:
“Congratulations {username}, you have successfully registered your account!”
 5. Authenticated users are redirected to the home view within 3 seconds after they close the
‘account creation’ message above.
 6. Account Creation is logged:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Business
 - e. Description
 - i. Feature: User Administration
 - ii. User Story ID: UA - 1
 - iii. Log Message: “Account with [Username] and [Email] successfully registered.”
 7. Registered user does not have access to registration view if currently authenticated.

Failure Outcomes:

1. Unregistered users encounter an error during registration, such as:
 - a. Invalid email:
 - i. The unregistered user is presented with an error message that says:
 1. “Invalid email provided. Retry again or contact the system administrator.”
 - ii. An invalid email error is logged in a persistent data store with:
 1. DateTime in UTC format
 2. Log Level: Warning
 3. Log Category: Business
 4. Log Message: “Invalid Email input: [email] ”
 - b. Duplicate email:
 - i. The unregistered user is presented with an error message that says:
 1. “Sorry this email is already being used, please try again with a different email.”
 - ii. A duplicate email error is logged in a persistent data store with:
 1. DateTime in UTC format
 2. Log Level: Warning
 3. Log Category: Business
 4. Log Message: “Email input already exists: [email]”
 - c. Inadequate password:
 - i. The unregistered user is presented with an error message that says:

1. "This password is inadequate: {explains what it is missing or needs to be removed to be adequate}."
 2. DateTime in UTC format
 3. Log Level: Warning
 4. Log Category: Business
 5. Log Message: "Inadequate Password input: ", with the password used.
- d. Invalid DOB:
- i. The unregistered user is presented with an error message that says:
 1. "Invalid date of birth provided. Must be within 1/1/1970 to Present."
 2. DateTime in UTC format
 3. Log Level: Warning
 4. Log Category: Business
 5. Log Message: "Date of Birth was invalid: ", along with the date inputted
- e. Email verification fails to deliver:
- i. The unregistered user is presented with an error message that says:
 1. "It looks like we were unable to send an email to that address! Please check that it is the correct email address and try again."
 2. System attempts to log confirmation email failure and records:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Debug
 - d. Log Category: Server
 - e. Log Message: "Confirmation email failed to send"
- f. Email verification expires after 2 hours:
- i. If unregistered user completes email confirmation after 2 hours:
 1. System displays "Confirmation time period has expired. Register again or contact the system administrator."
 2. A log is created and records:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Server
 - e. Log Message: "User completed email confirmation after it expired"
- g. Confirmed email before 2 hours, but system unable to assign unique username:
- i. The unregistered user is presented with an error that says:
 1. "Unable to assign username. Retry again or contact the system

- administrator.”
 - 2. The account is not created
 - ii. A log is created and records:
 - 1. DateTime in UTC format
 - 2. Username
 - 3. Log Level: Debug
 - 4. Log Category: Data Store
 - 5. Log Message: “Data store unable to assign unique username: [username]”
 - h. Creating an account takes longer than 3 seconds to complete:
 - i. Log will be recorded according to “Operation Time Limits” Default behavior
 - 1. Feature: User Administration
 - 2. Feature ID: UA - 1

UA-2 : As a registered user, I want to log in to my account to access registered user-specific content.

Complexity Level:

- Low
- Effort Points: 7

App Permissions:

-
- Permission:
 - Read
- Scope:
 - Read username in data store

Target Audience:

- Unauthenticated registered users who wish to log in to their Musi-Cali accounts.

Required Inputs:

- 1. Registered user email (3-254 Characters consisting of):
 - a. Must already exist in the data store.
 - b. Format: <valid_characters>@<valid_characters>
 - c. Case insensitive letters: a-z

- d. Numbers: 0-9
 - e. Symbols:
 - i. "._"
- 2. OTP (One-Time Password) as defined in NIST SP 800-63b section 5.1.4.1. It will be sent through to the registered account's email.
 - a. OTP expires every 3 minutes
 - b. Valid characters will consist of the following:
 - i. 0-9

Pre-Conditions:

- 1. Registered users have already created registered accounts.
- 2. Registered users are viewing and have access to the login page.

Success Outcomes:

- 1. Within 3 seconds of authenticating the registered user account the system redirects the authenticated user to their personalized home dashboard to access registered user content.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: info
 - iv. Log Category: view
 - v. Log Message: "Login to registered account was successful"

Failure Outcomes:

- 1. Invalid email:
 - a. The user is presented with a message saying "Invalid email."
- 2. Invalid OTP:
 - a. The user is presented with a message saying "Invalid One Time Password."
- 3. OTP expired:
 - a. The system displays a message to the user saying "Please generate a new code, this one has expired."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "User used expired OTP code."
- 4. Creating an account takes longer than 3 seconds to complete:
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Administration

ii. User Story ID: UA - 2

UA-3: As an authenticated user, I want to delete my account and all of its associated data.

Complexity Level:

- Low
- Effort Points: 7

App Permissions:

- Permission: Delete
- Scope: Delete registered account from data store

Target Audience:

- Any authenticated users who wish to delete their Musi-Cali accounts and all related data permanently.

Required Inputs:

- Email:
 - The email associated with the authenticated user's Musi-Cali account.
- Confirmation:
 - The user must click a button reading “Confirm” to delete their account.
- Cancellation
 - The user has the option to cancel the account deletion process at anytime.

Pre-Conditions:

1. The user must be authenticated.
2. The user is on delete account view.
3. User has permissions to delete account.
 - a. Only system administrators can delete other system administrator registered accounts.
4. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The authenticated user initiates the account deletion process by confirming their intention to delete the account using the “Confirm button”.
 - a. All PII data and user account data associated with the user's Musi-Cal account is permanently deleted.
2. The system displays a message saying “Account deletion successful”
 - a. Once the user acknowledges the message, within 3 seconds, they are navigated

back to the login view with default culture settings

3. A log is created and records:
 - a. DateTime in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Business
 - e. Log Message: “[Username]’s account was deleted”

Failure Outcomes:

1. Cancellation of deletion:
 - a. Authenticated users have the option to cancel the deletion process at any time before the final confirmation step.
2. User chooses to delete account and confirms action, but system does not delete both PII data or user account data.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Log Message: “Not all PII data or account data was deleted in account deletion”
3. Data is not permanently deleted from the system.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Log Message: “System failed to permanently delete account from system.”
4. System message does not show or shows erroneously “Account deletion successful’ after all PII data and user account data is permanently deleted from the system.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Log Message: “System failed to display successful account deletion message.”
5. The user is unable to acknowledge the system message “Account deletion successful”
 - a. A log is created and records:
 - i. DateTime in UTC format

- ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Log Message: “User unable to acknowledge account deletion”
- 6. The user is not automatically redirected to the default home view
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: View
 - v. Log Message: “Failed to navigate to home after account deletion”
- 7. The user is automatically redirected to the default home view, but the default language and culture setting is not shown
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data
 - v. Log Message: “Language and culture settings failed to revert to default”
- 8. The deletion process takes longer than 3 seconds to complete.
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: User Administration
 - ii. User Story ID: UA - 3

UA-4: As a registered user I want to recover access to an existing disabled account.

Complexity Level:

- Medium
- Effort points: 7

App Permissions:

- Permission:
 - Read
 - Create
- Scope:
 - Verify login credentials
 - Create Account Recovery Request

Target Audience:

- Any registered user with a disabled account.

Required Inputs:

- Username
 - This will be the registered user's email
 - (3-254 Characters consisting of):
 - Must already exist in the data store.
 - Format: <valid_characters>@<valid_characters>
 - Case insensitive letters: a-z
 - Numbers: 0-9
 - Symbols:
 - ". _"
- OTP
 - Must be a minimum of 8 characters:
 - Case insensitive letters: a-z
 - Numbers: 0-9

Pre-Conditions:

1. The registered user does not have an active authenticated session.
2. The registered user must be viewing and have access to the account recovery view.
3. Failure of this feature must not result in system going offline.

Success Outcomes:

1. Registered users provide valid username and OTP. The account recovery request is submitted to authorized system administrators within 3 seconds. A message displays "Account recovery request sent to system admin." within 3 seconds of executing the request.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "Account recovery request sent successfully"
2. Authenticated system admin reviews account recovery for registered users. A message displays "Account recovery completed for the user" within 3 seconds. Affected registered user regains access and can now authenticate.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info

- iv. Log Category: Business
- v. Log Message: "Account successfully recovered"

Failure Outcomes:

1. Invalid username or OTP
 - a. A message displays:
 - i. "Invalid username or OTP provided. Retry again or contact the system administrator."
2. Valid username but invalid OTP
 - a. A message displays:
 - i. "Invalid username or OTP provided. Retry again or contact the system administrator."
3. Valid username and OTP, but request is unavailable to system admin users.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Error Message: "Account recovery request unavailable to admin"
4. Registered user completes a valid account recovery request, but the message does not display within 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Administration
 - ii. User Story ID: UA - 4
5. Authorized admin user completes valid account recovery request, but message does not display within 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Administration
 - ii. User Story ID: UA - 4
6. Authorized admin user completes valid account recovery request, but message does not display within 3 seconds. Target user does not regain access.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Log Message: "User does not have access after account recovery"
7. Authorized admin user completes valid account recovery request, but message does not display within 3 seconds. Target user does not regain access within 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior

- i. Feature: User Administration
- ii. User Story ID: UA - 4

User Management:

Admin users have the ability to create, update, delete, disable, or enable any registered user account within the system. The system always has at least one system administrator account with total system access at all times. Only the system admins have access to view and perform the following user management functionalities.

UM-1 (Effort Points - 5): As a system administrator, I want to be able to create a new user account so that I can add new users to the system and grant them access.

Complexity Level:

- Medium
- Effort points: 9

App Permissions:

- Permission:
 - Read
 - Create
- Scope:
 - Verify login credentials
 - Create User Account

Target Audience:

- System administrators that are trying to create new user accounts within the system.

Required Inputs:

- Unique username (5-30 characters consisting of):
 - Must not be occupied by an already-existing user
 - Must not be nullable
 - Valid characters will consist of the following:
 - a-z
 - A-Z
 - 0-9
 - Special characters:

- .
- -
- @
- Unregistered user email (3-254 Characters consisting of):
 - Cannot already exist in the data store.
 - Format: <valid_characters>@<valid_characters>.<valid_characters>
 - Case insensitive letters: a-z
 - Numbers: 0-9
 - Symbols:
 - .
 - _
- First Name (2-25 Characters consisting of):
 - Case insensitive letters: a-z
- DOB (Valid dates include from 01/01/1970 to Present).

Optional Inputs:

- Last Name
 - Defaults to null.
 - 2-25 Characters consisting of:
 - Case insensitive letters: a-z
- Artist Occupation:
 - Defaults to null.
 - The user selects one of the following options for their artist portfolio:
 - Composer
 - Arranger
 - Producer
 - Instrumentalist
- Administrator:
 - Grants admin privileges.
 - Administrator accounts can only be created by other admin accounts.

Pre-Conditions:

1. The system administrator is logged into the system with an active authenticated session.
2. The system administrator is on the User Management view.
 - a. Only system administrators can access User Management view
3. The user has system administrator privileges.
4. The account email or unique username being created does not already exist in the data store.
5. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The system receives the user's request to create a new user account.
2. The new user account is successfully created in the system's data store in less than 3 seconds.
 - a. The system displays a system message indicating "UM operation was successful."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "New user account successfully created"

Failure Outcomes:

1. The provided account information already exists in the persistent data store.
 - a. System message is shown to the admin: "That account already exists, please try again"
2. The provided account information fails validation for correctness and completeness.
 - a. System message is shown to the admin: "Input invalid, please try again"
3. UM operation takes longer than 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Management
 - ii. User Story ID: UM - 1
4. UM operation completes within 3 seconds, but the system message does not appear or appears incorrectly.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Log Message: "UM operation did not show the expected system message"
5. UM operation completes within 3 seconds and accurately portrays the system message. However the latest data is not written to the data store.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data Store
 - v. Log Message: "UM operation failed to update the data store"

UM-2: As a system administrator, I want to be able to update an existing user account so that I can modify user information when necessary.

Complexity Level:

- High
- Effort Points: 10

App Permissions:

- Permission:
 - Read
 - Write
- Scope:
 - Verify valid unique username
 - Write edit information

Target Audience:

- System administrators that are trying to update existing user accounts within the system.

Required Inputs:

- Unique username (5-30 characters consisting of):
 - Must not be occupied by an already-existing user
 - Must not be nullable
 - Valid characters will consist of the following:
 - a-z
 - A-Z
 - 0-9
 - Special characters:
 - .
 - -
 - @
- Unregistered user email (3-254 Characters consisting of):
 - Cannot already exist in the data store.
 - Format: <valid_characters>@<valid_characters>.<valid_characters>
 - Case insensitive letters: a-z
 - Numbers: 0-9
 - Symbols:
 - .
 - -
 - _
- First Name (2-25 Characters consisting of):
 - Case insensitive letters: a-z

- DOB (Valid dates include from 01/01/1970 to Present).
- Last Name
 - Defaults to null.
 - 2-25 Characters consisting of:
 - Case insensitive letters: a-z
- Artist Occupation:
 - Defaults to null.
 - The user selects one of the following options for their artist portfolio:
 - Composer
 - Arranger
 - Producer
 - Instrumentalist

Pre-Conditions:

1. The system administrator is logged into the system with an active authenticated session.
2. The system administrator is on the User Management view.
3. The system administrator has system administrator privileges.
4. The request made to update is on an existing registered user account and adheres to input validation.
5. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The system receives the user's request to edit existing registered user information.
2. The new user account information is successfully written to the system's data store in less than 3 seconds.
 - a. The system displays a system message indicating "UM operation was successful."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "New user account information successfully written"

Failure Outcomes:

1. The provided account information does not exist in the persistent data store.
 - a. System message is shown to the admin: "That account does not exist, please try again"
2. The provided account information fails validation for correctness and completeness.
 - a. System message is shown to the admin: "Input invalid, please try again"
3. UM operation takes longer than 3 seconds.

- a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: User Management
 - ii. User Story ID: UM - 2
- 4. UM operation completes within 3 seconds, but the system message does not appear or appears incorrectly.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: “UM operation did not show the expected system message”
- 5. UM operation completes within 3 seconds and accurately portrays the system message. However the latest data is not written to the data store.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: “UM operation failed to update the data store”

UM-3: As a system administrator, I want to be able to delete a registered account, so that I can remove users from the system when required.

Complexity Level:

- Medium
- Effort Points: 5

App Permissions:

- Permission:
 - Read
 - Delete
- Scope:
 - Verify valid unique username
 - Delete registered account

Target Audience:

- System administrators that are attempting to delete existing user accounts from the system.

Required Inputs:

- Request to delete an existing user account.
 - Confirmation of request.
- Existing registered email

Pre-Conditions:

1. The system administrator is logged into the system with an active authenticated session.
2. The system administrator is on the User Management view.
3. The system administrator has system administrator privileges.
4. The request made to delete is on an existing registered user account.
5. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The system receives the user's request to delete an existing user account.
2. The system confirms the deletion action.
3. The user account is successfully removed from the system's data store in less than 3 seconds.
 - a. The system displays a system message indicating "UM operation was successful."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "New user account information successfully written"

Failure Outcomes:

1. The provided account information does not exist in the persistent data store.
 - a. System message is shown to the admin: "That account does not exist, please try again"
2. UM operation takes longer than 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Management
 - ii. User Story ID: UM - 3
3. UM operation completes within 3 seconds, but the system message does not appear or appears incorrectly.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Log Message: "UM operation did not show the expected system message"

4. UM operation completes within 3 seconds and accurately portrays the system message.
However the latest data is not written to the data store.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data Store
 - v. Log Message: "UM operation failed to update the data store"

UM-4: As a system administrator, I want to be able to disable an existing user account, so that I can temporarily restrict user access without permanent removal.

Complexity Level:

- Medium
- Effort Points: 5

App Permissions:

- Permission:
 - Read
 - Write
- Scope:
 - Read user's account details
 - Change the account status to a disabled account

Target Audience:

- System administrators that are seeking to disable a registered account..

Required Inputs:

- Request to disable an existing user enabled account.
 - Confirmation of request.
- Existing enabled registered email.

Pre-Conditions:

1. The system administrator is logged into the system with an active authenticated session.
2. The system administrator is on the User Management view.
3. The system administrator has system administrator privileges.
4. The request made to disable is on an existing enabled registered account.
5. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The system receives the user's request to disable an existing user account.
2. The system confirms the disabled action.
3. The user account is successfully disabled in the system's data store in less than 3 seconds.
 - a. The system displays a system message indicating "UM operation was successful."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Log Message: "New user account successfully disabled"

Failure Outcomes:

1. The provided account information does not exist in the persistent data store.
 - a. System message is shown to the admin: "That account does not exist, please try again"
2. UM operation takes longer than 3 seconds.
 - a. Log will be recorded according to "Operation Time Limits" Default behavior
 - i. Feature: User Management
 - ii. User Story ID: UM - 4
3. UM operation completes within 3 seconds, but the system message does not appear or appears incorrectly.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Log Message: "UM operation did not show the expected system message"
4. UM operation completes within 3 seconds and accurately portrays the system message. However the latest data is not written to the data store.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data Store
 - v. Log Message: "UM operation failed to update the data store"

UM-5: As a system administrator, I want to be able to enable a previously disabled user account through the account recovery request, so that I can restore user access.

Complexity Level:

- Low
- Effort Points: 6

App Permissions:

- Permission:
 - Read
 - Write
- Scope:
 - Read user's account recovery request
 - Change the account status to not disabled

Target Audience:

- System administrators that want to confirm or deny any account recovery requests.

Required Inputs:

- Account Recovery Request
 - Requires admin approval or denial of said request to either enable or disable selected account.

Pre-Conditions:

1. The system administrator is logged into the system with an active authenticated session.
2. The system administrator is on the User Management view.
3. The system administrator has system administrator privileges.
4. The request made to enable is on an existing disabled registered account.
5. Failure of this feature must not result in system going offline.

Success Outcomes:

1. The system receives the user's request to enable a previously disabled user account.
2. The system confirms the approval or denial action.
3. The user account's disabled status is successfully removed in the system's data store in less than 3 seconds.
 - a. The system displays a system message indicating "UM operation was successful."
 - b. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business

- v. Log Message: “User no longer disabled after account recovery request”

Failure Outcomes:

1. The provided account information does not exist in the persistent data store.
 - a. System message is shown to the admin: “That account does not exist, please try again”
2. UM operation takes longer than 3 seconds.
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: User Management
 - ii. User Story ID: UM - 5
3. UM operation completes within 3 seconds, but the system message does not appear or appears incorrectly.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Log Message: “UM operation did not show the expected system message”
4. UM operation completes within 3 seconds and accurately portrays the system message. However the latest data is not written to the data store.
 - a. A log is created and records:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data Store
 - v. Log Message: “UM operation failed to update the data store”

Usage Analysis Dashboard

The usage analysis dashboard is a view for accessing vital insights into registered user engagement with the Musi-Cali platform. This dashboard is for authenticated system administrators to view comprehensive data on login/registration attempts, and feature usage over different time spans.

UAD - 1: As an authenticated system administrator, I want to view a dashboard for displaying and gaining insights on registered user behaviors on the Musi-Cali App.

Complexity Level:

- Medium to High
- Effort points: 12

App Permissions:

- Permission: Read
- Scope: Authenticated user activity metrics

Target Audience:

- Any authenticated system administrator

Required Inputs:

- N/A

Pre-Conditions:

1. The system must be able to access the persistent data store
2. The user must be an authenticated system administrator
3. The user must be on the Usage Dashboard view

Success Outcomes:

1. The authenticated and authorized admin user is able to navigate to the usage dashboard view.
2. The dashboard is loaded within 15 seconds from the completion of navigation.
3. All of the following KPIs are successfully displayed on the dashboard:
 - a. Successful and failed login attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - b. Successful and failed registration attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - c. The top 3 longest page visits in seconds
 - i. Duration in seconds based on entry and exit is made for every page
 - d. The top 3 most used features in seconds
 - i. A count in seconds is made for every feature
 - e. Collaboration requests sent and accepted ratio
 - i. Successful view of the ratio of collab requests will be logged according to “Viewing” Default behavior
 - Feature: Usage Analysis Dashboard

- Feature ID: UAD - 1

4. All KPIs automatically refresh data every 60 seconds
 - a. Directly after the KPIs are refreshed, the system gives a small message to the authenticated system admin that “All KPIs are refreshed” with a timestamp indicator of the latest refresh.
5. A successful view of the usage analysis dashboard is logged in the following format
 - a. The date-time in the UTC format
 - b. Username of authenticated system admin
 - c. Log Level: Info
 - d. Log Category: Data Store
 - e. Log Description:
 - i. Feature: Usage Analysis Dashboard
 - ii. User Story ID: UAD - 1
 - iii. Log message: “Usage Analysis Dashboard view is successful”.
6. Any operation of the usage analysis dashboard doesn't lead to the system going offline.

Failure Outcomes:

1. The user is a system admin, but cannot navigate to the usage dashboard page, so the system presents an error message saying “The Usage Dashboard is not currently available, please try again”.
2. The Dashboard takes longer than 15 seconds to load upon completion of navigation
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Usage Analysis Dashboard
 - ii. Feature ID: UAD - 1
 - iii. Time limit changes:
 1. 15.1 -17 seconds is a default warning log
 2. 17.1 seconds and higher is a default error log
3. All of the KPI data takes longer than 60 seconds to refresh
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Usage Analysis Dashboard
 - ii. Feature ID: UAD - 1
 - iii. Time limit changes:
 1. 60.1 - 62 seconds is a default warning log
 2. 62.1 seconds and higher is a default error log

4. Any of the following KPIs have failed to be displayed on the dashboard:
 - a. Successful and failed login attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 1
 - b. Successful and failed registration attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 1
 - c. The top 3 longest page visits in seconds
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 1
 - d. The top 3 most used features in seconds
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 1
 - e. Collaboration requests sent and accepted ratio
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 1

UAD - 2 : As an authenticated system administrator on the Dashboard View, I want to change the time period for viewing sets of data on registered user behaviors on the Musi-Cali App.

Complexity Level:

- Medium to High
- Effort points: 12

Required Inputs:

- Selection of any of the following criteria for filtering the data of registered user behaviors:
 - 6 months
 - 12 months
 - 24 months

App Permissions:

- Permission: Read
- Scope: Authenticated user activity metrics

Target Audience:

- Any authenticated system administrator

Pre-Conditions:

1. The system must be able to access the persistent data store
2. The user must be an authenticated system administrator
3. The user must be on the Usage Dashboard view
4. The user must be on the Usage Dashboard time span selection screen

Success Outcomes:

1. The authenticated and authorized admin user is able to navigate directly to the usage dashboard time span selection screen, where it loads upon 3 seconds of invocation
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Usage Analysis Dashboard
 - ii. Feature ID: UAD - 2
2. The authenticated system admin is able to choose 6, 12, or 24 months for usage analysis.
3. All of the following KPIs are successfully displayed on the dashboard within a view of 6 months, 12 months, or 24 months :
 - a. Successful and failed login attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - b. Successful and failed registration attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - c. The top 3 longest page visits in seconds
 - i. Duration in seconds based on entry and exit is made for every page
 - d. The top 3 most used features in seconds
 - i. A count in seconds is made for every feature
 - e. Collaboration Search user requests sent and accepted ratio
 - i. Successful view of the ratio of collab requests will be logged according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard

2. Feature ID: UAD - 2

Failure Outcomes:

1. The authenticated and authorized admin user is able to navigate directly to the usage dashboard time span selection screen, where it loads longer than 3 seconds of invocation
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Usage Analysis Dashboard
 - ii. Feature ID: UAD - 2
2. The authenticated system admin is unable to choose between 6, 12, or 24 months for the usage analysis.
 - a. The system presents an error message: “Time span selection for __ (6, 12, or 24) months is currently unavailable.”
 - b. Log will be recorded according to “Viewing” Default behavior
 - i. Feature: Usage Analysis Dashboard
 - ii. Feature ID: UAD - 2
3. Any of the timespans (6 months, 12 months, 24 months) have failed to display any of the following KPIs on the dashboard:
 - a. Successful and failed login attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 2
 - b. Successful and failed registration attempts represented per month within the chosen time span of 6, 12, or 24 months in a trend chart
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 2
 - c. The top 3 longest page visits in seconds
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 2
 - d. The top 3 most used features in seconds
 - i. Log will be recorded according to “Viewing” Default behavior
 1. Feature: Usage Analysis Dashboard
 2. Feature ID: UAD - 2
 - e. Collaboration requests sent and accepted ratio
 - i. Log will be recorded according to “Viewing” Default behavior

1. Feature: Usage Analysis Dashboard
2. Feature ID: UAD - 2

User Privacy Control

This system requirement makes it so that any authenticated user's private data is protected and not accessible by anyone other than the administrator and owner of that private data.

UPC-1: As an authenticated user, I want to see what data has been collected on me.

Complexity Level:

- Medium
- Effort Points: 8

App Permissions:

- Permissions:
 - Read
- Scope:
 - The authenticated user must have read permissions to see the data collected from them by the system.

Target Audience:

- Any authenticated talent or admin user that wants to view the data the system has collected on their registered accounts.

Required Inputs:

- Authentication credentials in order to access the data that has been collected
 - Username and OTP

Optional Inputs:

- Navigate to account deletion, refer to UA-3.

Pre- Conditions:

- Must adhere to EULA per GDPR or California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA).
- Must be authenticated an authenticated talent or admin user.
- Must be on privacy view.

- Must be able to navigate to account deletion view, refer to UA-3.

Success Outcomes:

1. User is able to see any and all data that they have given to the app
 - a. Includes sensitive information:
 - i. PII Data: Government Name, City, Zip Code, Street Address
2. Any data that is shown to the user is up-to-date and accurate
3. A successful view of the User Privacy Control is logged in the following format:
 - a. The DateTime in UTC format
 - b. Username of authenticated system admin
 - c. Log Level: Info
 - d. Log Category: Data Store
 - e. Log Description:
 - i. Feature: User Privacy Control
 - ii. User Story ID: UPC - 1
 - iii. Log message: "User Privacy Control view is successful".
4. User is able to navigate to account deletion UA-3 view.

Failure Outcomes:

1. User is unable to see the data that they have given the app
 - a. If this happens, the time of this error happening will be logged
 - b. This error log will create these records:
 - i. Datetime in UTC format
 - ii. Username and OTP of authenticated system admin
 - iii. Log Level: Error
 - iv. Log Category: View
 - v. Description
 1. Feature: User Privacy Control
 2. User Story ID: UPC-1
 3. Error Message: "User is unable to view their data."
2. User can view another authenticated user's data
 - a. If this happens, the system will print out an error saying, "User was able to view another user's data."
 - b. This error log is created that records:
 - i. Datetime in UTC format
 - ii. Username and OTP of authenticated system admin
 - iii. Log Level: Error

- iv. Log Category: Data
 - v. Description
 - 1. Feature: User Privacy Control
 - 2. User Story ID: UPC-1
 - 3. Error Message: “User is able to view another user’s data.”
3. User can delete another authenticated user’s account
- a. If this happens, the system will print out an error saying, “User was able to delete another user’s data.”
 - b. This error log is created that records:
 - i. Datetime in UTC format
 - ii. Username and OTP of authenticated system admin
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Description
 - 1. Feature: User Privacy Control
 - 2. User Story ID: UPC-1
 - 3. Error Message: “User can delete another user’s account.”

Phase 1 Feature Requirements

Artist Portfolio:

The Artist Portfolio will be a personalized collection for authenticated users to display their tracks, clips, demos, and a specified occupation of either composer, arranger, producer, instrumentalist or “none” to other authenticated users.

AP - 1: As an authenticated user, I want to successfully upload a self description, audio tracks, clips, or demos to show on my portfolio.

Complexity Level:

- Medium to high
- Effort points: 7

App Permissions:

- Permission: Write
- Scope: Write to portfolio

Target Audience:

- Any talent role or admin role users

Required Inputs:

- Audio tracks, clips, or demos in supported formats (.mp3, .wav, .mp4)
 - Max Length of Audio File: 8 minutes
 - Upload amount: 1 file at a time

Optional Inputs:

- Metadata for each uploaded item (title, description, genre)
 - Default Title: filename of uploaded file
 - 3-30 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Numbers: 0-9
 - Symbols: "@._!'?^{}~"
 - Default Description: Null
 - 3-254 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Numbers: 0-9
 - Symbols: "@._!'?^{}~"
 - Default Genre: Null
 - 3-30 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Symbols: "@._!'?^{}~"
 - Default Description: Null
 - 3-254 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z

- Symbols: "@._!'^{}~"

Pre-Conditions:

1. User must be authenticated
2. Authenticated users are on their portfolio creating/editing interface.

Success Outcomes:

1. The Authenticated user successfully uploads audio tracks, clips, or demos to their portfolio.
 - a. Uploaded items are stored securely in the system's persistent data store in 3 seconds.
 - b. Metadata associated with each item (optionally provided description, track name, genre) is saved to the database, attached to the user that uploaded the file and the metadata is displayed when looking at the file's info. File is only accessible under that User's Portfolio
 - c. The authenticated user receives a confirmation message indicating successful uploads.
2. A log is created when a user successfully uploads a file that records:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Data
 - e. Description
 - i. Feature: Artist Portfolio
 - ii. User Story ID: AP - 1
 - iii. Log Message: "User has successfully uploaded a audio file"

Failure Outcomes:

1. The Authenticated user encounters an error during the upload process (ex. Formatting errors with metadata, or being unable to save to the database), resulting in failed uploads, and then the system logs the error for a timestamp and details of the issue.
 - a. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 1
 3. Error Message: "Audio file was not able to be uploaded"

2. The uploaded items are not stored in the system's persistent data store within 3 seconds
 - a. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Artist Portfolio
 - ii. Feature ID: AP - 1
3. If an uploaded file format is not supported (e.g., not .mp3, .wav, or .mp4), the system displays “File uploaded is not supported, please choose another (.mp3, .wav, .mp4),” and the upload attempt fails.
 - a. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Data
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 1
 3. Error Message: “File uploaded is not supported”
4. If the app experiences technical difficulties during the upload process, such as server issues or connectivity problems, the user receives an error message saying, “There was a problem with the server connection, please try again later.”
 - a. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Server
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 1
 3. Error Message: “There was a problem with the server connection”

AP - 2: As an authenticated user, I want to change my artist occupation (composer, arranger, producer, instrumentalist, none) in my portfolio for accuracy in collaboration.

Complexity Level:

- Medium to high
- Effort points: 4

App Permissions:

- Permission: Read-Write
- Scope: Portfolio Management

Target Audience:

- Any Talent Role or Admin Role users

Required Inputs:

- Selection of a new artist occupation (composer, arranger, producer, or instrumentalist)

Pre-Conditions:

1. The authenticated user must be logged in with valid credentials.
2. Authenticated users are on their portfolio editing interface.

Success Outcomes:

1. The authenticated user successfully selects and changes their artist occupation within the portfolio.
 - a. A successful occupation change is logged with the format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 2
 3. Log Message: "Successful portfolio occupation change"
2. The updated artist's occupation is securely stored in the system's relational database.
 - a. A successful storage of the occupation is logged with the format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Data
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 2
 3. Log Message: "[Occupation] successfully stored."
3. The authenticated user receives a confirmation message confirming the successful change of artist occupation, "Occupation changed."

Failure Outcomes:

1. The authenticated user encounters an error during the occupation change process, resulting in a failed update.
 - a. The system logs the error for a timestamp and details of the issue.
 - i. A log is created that records:
 1. Date and time in UTC format

2. Username
3. Log Level: Error
4. Log Category: Data
5. Description
 - a. Feature: Artist Portfolio
 - b. User Story ID: AP - 2
 - c. Error Message: "Occupation change unable to be made."

AP - 3: As an authenticated user, I want to set the visibility of my portfolio to public, private, or selective to control who can access my shared content

Complexity Level:

- Medium to high
- Effort points: 4

App Permissions:

- Permission: Read-Write
- Scope: Portfolio Management

Target Audience:

- Any Talent Role or Admin Role users

Required Inputs:

- Selection of visibility settings (public, private, or selective)

Optional Inputs:

- Selection of specific users (for selective visibility)

Pre-Conditions:

1. The authenticated user must be logged in with valid credentials.
2. The authenticated user is accessing their portfolio settings or editing interface.

Success Outcomes:

1. The authenticated user successfully sets the visibility of their portfolio to one of the available options (public, private, or selective).
 - a. The authenticated user receives a confirmation message indicating the successful change in visibility settings.
 - b. A successful portfolio visibility change is logged with the format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business

- v. Description
 - 1. Feature: Artist Portfolio
 - 2. User Story ID: AP - 3
 - 3. Log Message: "Portfolio changed to [selected visibility option]."
- 2. Portfolio visibility status is stored in the system's database.
 - a. A visibility status being stored is logged with the format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Data
 - v. Description
 - 1. Feature: Artist Portfolio
 - 2. User Story ID: AP - 3
 - 3. Log Message: "Visibility Status stored."

Failure Outcomes:

- 1. The user encounters an error, causing the portfolio visibility to not be applied
 - a. The system logs the error for a timestamp and details of the issue.
 - i. A log is created that records:
 - 1. Date and time in UTC format
 - 2. Username
 - 3. Log Level: Error
 - 4. Log Category: Data
 - 5. Description
 - a. Feature: Artist Portfolio
 - b. User Story ID: AP - 3
 - c. Error Message: "Portfolio visibility not able to be applied."
- 2. The user is immediately notified of the failure with a clear error message, "Portfolio visibility error, please try again."

AP - 4 : As an authenticated user, I want to view other registered users' public portfolios to explore possible collaboration opportunities.

Complexity Level:

- Medium to high
- Effort points: 5

App Permissions:

- Permission: Read
- Scope: Portfolio exploration

Target Audience:

- Any Talent Role or Admin Role user

Required Inputs:

- Selection of any public registered user whose portfolio to view

Pre-Conditions:

1. The authenticated user must be logged in with valid credentials.
2. The authenticated user is accessing the portfolio viewing interface.
3. The authenticated user has selected another registered user's portfolio to view.

Success Outcomes:

1. The authenticated user can access and view the selected user's public portfolio.
 - a. Log will be recorded according to "Viewing" Default behavior
 - i. Feature: Artist Portfolio
 - ii. Feature ID: AP - 4
2. The portfolio content is displayed in a user-friendly format, showing audio tracks, clips, and demos, where the user can navigate and listen to all of the selected portfolio's content.
 - a. This is logged with the format:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 1. Feature: Artist Portfolio
 2. User Story ID: AP - 4
 3. Log Message: "Portfolio listening is fully successful."

Failure Outcomes:

1. The authenticated user encounters an error while trying to access or view the selected portfolio, so the system will give an error message "The portfolio is currently unavailable".
 - a. The system logs the error for a timestamp and details of the issue.
 - i. A log is created that records:
 1. Date and time in UTC format
 2. Username
 3. Log Level: Error
 4. Log Category: Data
 5. Description
 - a. Feature: Artist Portfolio

- b. User Story ID: AP - 4
- c. Error Message: “Viewing this portfolio is currently unavailable, please try again..”

Artist Profile Calendar:

The artist profile calendar is a calendar on an artist’s profile where other users can view the artist’s upcoming gigs.

APC - 1: As an authenticated user, I want to post upcoming gigs on my profile calendar.

Complexity Level:

- High
- Effort Points: 8

App Permissions:

- Permission:
 - Write
- Scope:
 - Write gigs to future calendar dates.

Target Audience:

- Any authenticated talent or admin user that wants to post future gigs to their profile calendar.

Required Inputs:

- “Post gig” Option:
 - Lets the user choose gigs to post to their profile calendar

Pre-Conditions:

1. User must be an authenticated user
2. Authenticated users are in their profile calendar

Success Outcomes:

1. The authenticated user is able to post a gig to their profile calendar.
 - a. The system will display a message saying “Successfully posted [gig] to your

- profile calendar”
- b. Successful posting of gig is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 1
 - Log Message: “Gig was successfully added to the profile calendar”

Failure Outcomes:

- The gig is unable to be added to the artist profile calendar:
 - The authenticated user is presented with an error message that says:
 - “Sorry, the gig was unable to be added to the profile calendar.”
 - Error is logged in a persistent data store:
 - Date and time in UTC format
 - Username
 - Log Level: Error
 - Log Category: Server
 - Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 1
 - Log Message: “Gig failed to be added to the profile calendar”
- Adding a gig to the profile calendar takes longer than 3 seconds

APC - 2: As an authenticated user, I want to set the visibility of my gig listings to public or private.

Complexity Level:

- Medium
- Effort Points: 7

App Permissions:

- Permission: Write
- Scope: edit gig visibility

Target Audience:

- Any authenticated talent or admin user who wants to change the visibility of their profile calendar

Required Inputs:

- “Public” Option:
 - Anybody may view the profile calendar
- “Private” Option:
 - Only the authenticated user may view the profile calendar
- Defaults to public

Pre-Conditions:

1. Registered users must log in with the correct credentials.
2. Must be on the Artist Portfolio calendar page

Success Outcomes:

1. The authenticated user is able to change the visibility of their profile calendar.
 - a. The system will display a message saying “Successfully set your profile calendar visibility to [option]”
 - b. Successful edit of artist portfolio visibility is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 2
 - Log Message: “Artist portfolio visibility was successfully set.”

Failure Outcomes:

- Authenticated user encounters an error when trying to change profile calendar visibility:
 - The authenticated user is presented with an error message that says:
 - “Sorry, the profile calendar visibility was unable to be changed.”
 - Error is logged in a persistent data store:
 - Date and time in UTC format
 - Username
 - Log Level: Error
 - Log Category: Data
 - Description

- Feature: Artist Profile Calendar
- User Story ID: APC - 2
- Log Message: "Privacy settings failed to update"
- Changing profile calendar visibility takes longer than 3 seconds.

APC - 3: As an authenticated user, I want to edit the gigs I have created.

Complexity Level:

- High
- Effort Points: 9

App Permissions:

- Permission:
 - Write
- Scope:
 - Edit gig in calendar

Target Audience:

- Any authenticated talent or admin user who wants to edit their gigs.

Required Inputs:

- "Edit gig" option:
 - Allows authenticated users to edit gig data such as:
 - Name
 - 3-254 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Symbols: "@._-!#\$%`*+/?^'{}|~"
 - Location
 - 3-254 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Numbers: 0-9
 - Symbols: "@._-!#\$%`*+/?^'{}|~"
 - Time
 - Who is performing
 - 3-254 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z

- Symbols: "@._-!#\$%`*+/?^'{}|~"

Pre-Conditions:

1. User must be authenticated.
2. User must be viewing a gig on the profile calendar.
3. User must have access to edit functionality.

Success Outcomes:

1. The authenticated user is able to edit their gig.
 - a. The system will display a message saying "Successfully edited gig on calendar"
 - b. Successful edit of artist calendar gig is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 3
 - Log Message: "User edited gig on calendar"

Failure Outcomes:

- Authenticated user encounters an error when trying to edit gig data:
 - The authenticated user is presented with an error message that says:
 - "Sorry, the changes to gig data could not be saved."
 - Error is logged in a persistent data store:
 - Date and time in UTC format
 - Username
 - Log Level: Error
 - Log Category: Data
 - Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 3
 - Log Message: "Unable to edit gig data"

APC - 4: As an authenticated user, I want to delete the gigs I have created.

Complexity Level:

- Low

- Effort Points: 5

App Permissions:

- Permission:
 - Delete
- Scope:
 - Remove gig from calendar

Target Audience:

- Any authenticated talent or admin user who wants to delete their gigs.

Required Inputs:

- “Delete gig” option
 - Allows authenticated users to delete gigs.
 - Authenticated users will be asked “Are they sure that they want to delete this gig?” after choosing this option.

Pre-Conditions:

1. User must be authenticated.
2. Authenticated users must be viewing a gig on the profile calendar.
3. User must have access to gig delete functionality

Success Outcomes:

1. The authenticated user is able to delete their gig.
 - a. The system will display a message saying “Successfully deleted gig on calendar”
 - b. Successful delete of artist calendar gig is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 1. Feature: Artist Profile Calendar
 2. User Story ID: APC - 4
 3. Log Message: “User deleted gig on calendar”

Failure Outcomes:

- Authenticated user encounters an error when trying to delete a gig:
 - The authenticated user is presented with an error message that says:
 - “Sorry, the gig could not be deleted.”
 - Error is logged in a persistent data store:

- Date and time in UTC format
- Username
- Log Level: Error
- Log Category: Data Store
- Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 4
 - Log Message: “Gig failed to be deleted”
- Deleting a gig takes longer than 3 seconds.

APC- 5: As an authenticated user, I want to view other registered users gig listings and details.

Complexity Level:

- High
- Effort Points: 8

App Permissions:

- Permission: Read
- Scope: find gigs

Target Audience:

- Any authenticated talent or admin user that wants to view a gig on a registered user’s profile calendar.

Required Inputs:

- “Gig highlighting”
 - Will display the data of a gig the user has selected

Pre-Conditions:

1. The authenticated user must be logged in and authenticated.

Success Outcomes:

1. The authenticated user is able to view the profile calendar.
 - a. Successful view of artist calendar is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business

- v. Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 5
 - Log Message: ““Successfully viewed another user’s profile calendar””
- 2. The authenticated user is able to view gigs and their data.
 - a. The system will a display a message saying “Successfully highlighted gig on calendar”
 - b. Successful delete of artist calendar gig is logged in a persistent data store:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Info
 - iv. Log Category: Business
 - v. Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 5
 - Log Message: “User highlighted gig on [username]’s calendar”

Failure Outcomes:

- Authenticated user encounters an error when trying to display the profile calendar:
 - The authenticated user is presented with an error message that says:
 - “Sorry, the profile calendar could not be displayed.”
 - Error is logged in a persistent data store:
 - Date and time in UTC format
 - Username
 - Log Level: Error
 - Log Category: View
 - Description
 - Feature: Artist Profile Calendar
 - User Story ID: APC - 4
 - Log Message: “Failed to display the Artist Profile Calendar”
- Authenticated user encounters an error when trying to view gig data:
 - The authenticated user is presented with an error message that says:
 - “Sorry, the gig data could not be displayed.”
 - Error is logged in a persistent data store:
 - Date and time in UTC format
 - Username
 - Log Level: Error
 - Log Category: Data Store
 - Description

- Feature: Artist Profile Calendar
- User Story ID: APC - 4
- Log Message: “Failed to retrieve gig data from the data store”
- Displaying the profile calendar takes longer than 3 seconds.
- Viewing gig data takes longer than 3 seconds.

Collaboration Search:

Authenticated users will be able to search for registered users to potentially start a collaboration on a cover project.

CS-1: As an authenticated user, I want to change my personal search visibility flag setting to manage my visibility for collaboration opportunities.

Complexity Level:

- Medium.
- Effort Points: 6

App Permissions:

- Permission: Write
- Scope: Search visibility

Target Audience:

- Any Talent role users

Required Inputs:

- User search visibility preference
 - Enabling this setting grants authenticated users permission to search for other registered users using filters and also makes them discoverable to other registered users.
 - Disabling this setting will make the authenticated user incapable of using the collaboration search feature and undiscoverable to other registered users using the search feature.

Pre-Conditions:

1. Users must be authenticated.
2. The authenticated user must have created an account with a valid email and username.

3. The authenticated user must have chosen an occupation.
4. The user must be viewing the visibility flag setting.

Success Outcomes:

1. The authenticated user successfully shows up in the search results if they have this setting enabled.
2. The authenticated user does not show up in the search results if they have this setting disabled.
3. A log is created after the user has changed their user visibility preference that records:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: View
 - e. Description
 - i. Feature: Collaboration Search
 - ii. User Story ID: CS - 1
 - iii. Log Message: "User has enabled/disabled "

Failure Outcomes:

1. The authenticated user does not show up in the search results if they have this setting enabled.
 - a. If this happens, the system will print an error message saying, "Please Be Sure To Save Your Settings," and then prompt the user to return to their profile to update their Collaboration Search settings.
 - b. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: View
 - v. Description
 1. Feature: Collaboration Search
 2. User Story ID: CS - 1
 3. Error Message: "User is not visible with Collaboration search visibility flag toggled on"
2. The authenticated user shows up in the search results if they have this setting disabled.
 - a. If this happens, the system will print an error message saying, "Please Be Sure to Save Your Settings," and then prompt the user to return to their profile to update their Collaboration Search settings.
 - b. A log is created that records:
 - i. Date and time in UTC format

- ii. Username
- iii. Log Level: Warning
- iv. Log Category: View
- v. Description
 - 1. Feature: Collaboration Search
 - 2. User Story ID: CS - 1
 - 3. Error Message: “User is visible with Collaboration search visibility flag toggled off”
- 3. Updating the search visibility flag setting takes longer than 3 seconds to complete.
 - a. System will display a message to the user saying: “System Error: Task Not Completed In Time,” and prompt the user to go back to the previous page and try using the Collaboration Search again.
 - b. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Collaboration
 - ii. Feature ID: CS - 1

CS-2: As an authenticated user, I want to locate other authenticated users to collaborate with.

Complexity Level:

- High.
- Effort Points: 6

App Permissions:

- Permissions: Read
- Scope: Read User Data

Target Audience:

- Any Talent role users.

Required Inputs:

- “Start Search” option
 - With this option, the app locates other authenticated users
- “Stop Search” option
 - With this option, the app cancels the search and returns the user to the collaboration search view.

Pre-Conditions:

1. Users must be authenticated.
2. The authenticated user must have created an account with a valid email and username.

3. The authenticated user must have chosen an occupation.
4. The user must be viewing the collaboration search setting.

Success Outcomes:

1. The authenticated user is successfully able to find other authenticated users after choosing the “Start Search.”
2. The authenticated user is successfully able to stop finding other authenticated users after choosing the “Stop Search.”
3. A log is created after the user has found other musician within 3 seconds:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: View
 - e. Description
 - i. Feature: Collaboration Search
 - ii. User Story ID: CS - 2
 - iii. Log Message: “User has found other musicians”

Failure Outcomes:

1. The authenticated user cannot find other users after choosing the “Start Search” option.
 - a. If this happens, the system will print an error message saying, “Be sure to set an occupation on your profile.” Then prompt the user to go back to the profile view and update their settings.
 - b. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: View
 - v. Description
 1. Feature: Collaboration Search
 2. User Story ID: CS - 2
 3. Error Message: “User cannot find other users after choosing ‘Start Search.’”
2. The authenticated user cannot stop finding other authenticated users after choosing the “Stop Search” option.
 - a. If this happens, the system will print an error message saying, “System Error: Please select “Stop Search” again.”
 - b. A log is created that records:
 - i. Date and time in UTC format
 - ii. Username

- iii. Log Level: Error
- iv. Log Category: Server
- v. Description
 - 1. Feature: Collaboration Search
 - 2. User Story ID: CS - 2
 - 3. Error Message: “User cannot stop the search process after selecting ‘Stop Search.’”
- 3. Updating the user’s occupation takes longer than 3 seconds to complete.
 - a. System will display a message to the user saying: “System Error: Task Not Completed In Time,” and prompt the user to go back to the previous page and try using the Collaboration Search again.
 - b. Log will be recorded according to “Operation Time Limits” Default behavior
 - i. Feature: Collaboration
 - ii. Feature ID: CS - 2

Collab Feature:

- This feature allows authenticated users to request and accept collaboration

CF-1: As an authenticated user, I want to send collaboration requests to other authenticated users.

Complexity Level:

- High
- Effort Points: 10

App Permissions:

- Permissions: Create and Write permissions
- Scope: Creating a new collaboration request and being able to edit that request

Target Audience:

- Talent and Admin user roles

Required Inputs:

- Authenticated users sending a collaboration request need to send a description of their project.
 - The description will consist of:
 - 3-300 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Numbers: 0-9
 - Symbols: "@._-!#`*+/?^'{}|~"
- Authenticated users who send a request to a talent of interest are asked by the app what they want the talent of interest to do in their collaboration.
 - The user's wants will consist of:
 - 3-300 Characters consisting of:
 - Uppercase letters: A-Z
 - Lowercase letters: a-z
 - Numbers: 0-9
 - Symbols: "@._-!#`*+/?^'{}|~"

Pre-Conditions:

1. Users must be authenticated.
2. An authenticated user must be on the collaboration request page.

Success Outcomes:

1. The authenticated user's collaboration request is sent to the talent of interest within 3 seconds.
2. The authenticated user's collaboration request is saved by the system after
3. The authenticated user is able to send the collaboration request to the talent of interest.
4. The talent of interest is able to receive collaboration requests from an authenticated user.
5. The talent of interest is able to view collaboration requests from an authenticated user.
6. The talent of interest is able to accept collaboration requests from an authenticated user by choosing the "Accept Request" option.
7. The talent of interest is able to decline collaboration requests from an authenticated user by choosing the "Decline Request" option.
8. A log is created when an authenticated user creates a new collaboration request:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Data
 - e. Description

- i. Feature: Collab Feature
- ii. User Story ID: CF - 1
- iii. Log Message: "{Username} has sent a collaboration request to {Username}"

Failure Outcomes:

- The authenticated user's request is not sent.
 - In response, the system will print an error message saying, "Collaboration Request Failed to Send. Please Try Again."
 - Error is logged:
 - DateTime in UTC format
 - Username
 - Log Level: Error
 - Log Category: Data
 - Description
 - Feature: Collab Feature
 - User Story ID: CF - 1
 - Error Message: "Collab Request failed to send"
- The authenticated user's request is not visible by the talent of interest.
 - In response, the system will fetch the text file of the message in the database and prompt the user that sent it to resend the request.
 - Error is logged:
 - DateTime in UTC format
 - Username
 - Log Level: Error
 - Log Category: View
 - Description
 - Feature: Collab Feature
 - User Story ID: CF - 1
 - Error Message: "Error loading Collab Request"
- The description is under 3 characters long or over 300 characters long.
 - In response to being under 3 characters, the system will print an error message saying, "Description Value Must Be Longer."
 - In response to being over 300 words, the system will print an error message saying, "Description Value Must Under 300 Words."
 - Error is logged:
 - DateTime in UTC format
 - Username
 - Log Level: Warning

- Log Category: Data
- Description
 - Feature: Collab Feature
 - User Story ID: CF - 1
 - Error Message: “Invalid description length”
- The description contains characters that are not specified to be accepted.
 - In response, the system will print an error message saying, “Description Includes Characters That Are Not Accepted.”
 - Then the system will display the characters that aren’t accepted so that the user can remove them from the description.
 - Error is logged:
 - DateTime in UTC format
 - Username
 - Log Level: Warning
 - Log Category: Data
 - Description
 - Feature: Collab Feature
 - User Story ID: CF - 1
 - Error Message: “Invalid characters used”
- The authenticated user’s request is not saved to the internal database.
 - In response, the system will print an error message saying, “Error: Request Not Saved. Please Select ‘Save As Draft’ Before Closing Next Time.”

CF-2: As an authenticated user, I want to view incoming collaboration requests and decide whether to accept or decline them.

Complexity Level:

- Medium
- Effort Points: 3

App Permissions:

- Permissions: Read and Delete permissions
- Scope: Read permissions in order to see the collaboration request and Delete permissions in order to delete the collaboration request after the request has been accepted or denied

Target Audience:

- Talent and Admin role users

Required Inputs:

- Authenticated users can view collaboration requests from other authenticated users.
- Authenticated users can either accept or decline collaboration requests from other authenticated users.

Pre-Conditions:

1. Users must be authenticated.
2. The authenticated user is on the collaboration request page.
3. The authenticated user must have received collaboration requests from other authenticated users.

Success Outcomes:

1. The authenticated user is able to access the collaboration request within 3 seconds of receiving the message.
2. A log is created when an authenticated user accepts or declines a collaboration request:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Data
 - e. Description
 - i. Feature: Collab Feature
 - ii. User Story ID: CF - 2
 - iii. Log Message: "{Username} has accepted/declined {Username}'s request"

Failure Outcomes:

1. The authenticated user is unable to access the collaboration request within 3 seconds.
 - a. Error is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Description
 1. Feature: Collab Feature
 2. User Story ID: CF - 2
 3. Error Message: "Unable to access request in 3 seconds"
2. The authenticated user is unable to accept or decline collaboration requests.

- a. System messages user saying, “Collaboration request was unable to be accepted/declined, please try again later.”
- b. If the collaboration request is declined, the authenticated user that sent the request is not notified within 3 seconds.
 - i. The collaboration request data is not deleted from the database within 3 seconds.
- c. If the collaboration request is accepted, the authenticated user that sent the request is not notified within 3 seconds.
- d. Error is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Data
 - v. Description
 - 1. Feature: Collab Feature
 - 2. User Story ID: CF - 2
 - 3. Error Message: “Unable to accept/decline collaboration request”

CF-3: As an authenticated user, I want to cancel my collaboration request.

Complexity Level:

- Medium
- Effort Points: 3

App Permissions:

- Permissions: Read and Delete permissions
- Scope: Read the collaboration request and delete the request the authenticated user made

Target Audience:

- Talent and Admin role users

Required Inputs:

- Authenticated users select to cancel their collaboration request.

Pre-Conditions:

1. User must be authenticated
2. The authenticated user must be on the collaboration request page.
3. Authenticated users had already sent a collaboration request to another authenticated user.
4. The collaboration request had not been accepted or declined.

Success Outcomes:

1. The collaboration request data is deleted from the internal database within 3 seconds.
2. The authenticated user who received the collaboration request can no longer see the request after the data has been deleted.
3. A log is created after the user deletes their collaboration request:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: Data
 - e. Description
 - i. Feature: Collab Feature
 - ii. User Story ID: CF - 3
 - iii. Log Message: "{Username} has deleted their collaboration request"

Failure Outcomes:

1. The collaboration request data is not deleted from the internal database within 3 seconds.
 - a. Error is logged:
 - i. DateTime in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Business
 - v. Description
 1. Feature: Collab Feature
 2. User Story ID: CF - 3
 3. Error Message: "Unable to delete collaboration request in 3 seconds"
2. The authenticated user who received the collaboration request can still see the request after the data has been deleted.
 - a. Error is logged:

- i. DateTime in UTC format
- ii. Username
- iii. Log Level: Error
- iv. Log Category: View
- v. Description
 1. Feature: Collab Feature
 2. User Story ID: CF - 3
 3. Error Message: "Error deleting collaboration request"

Bingo Board:

The Bingo Board is a place for authenticated users, usually venues, to post available gigs for other authenticated users to apply to.

BB - 1: As an authenticated user, I can make a post to the bingo board that other authenticated users will see.

Complexity Level:

- Low
- Effort points: 6

App Permissions:

- Permission: Create
- Scope: Gig posting

Target Audience:

- Authenticated talent or admin users who are looking to hire artists for gigs or other work.

Required Inputs:

- Authenticated users input information for the gig:
 - Name of the Gig:
 - 3-50 characters:
 - Lower Case: a-z
 - Upper Case: A-Z
 - Numbers: 0-9
 - Symbols: "@._!'?^{}~"

Optional Inputs:

- Additional information about the gig:
 - A general description:
 - Default: Null
 - 0-1000 characters:
 - Lower Case: a-z
 - Upper Case: A-Z
 - Numbers: 0-9
 - Symbols: "@._!'?^{}~"
 - Gig Location:
 - Default: Null
 - Optional setting: Online/Asynchronous
 - 0-50 characters:
 - Lower Case: a-z
 - Upper Case: A-Z
 - Numbers: 0-9
 - Symbols: "@._!'?^{}~"
 - Date:
 - Default: Null
 - A date formatted with MM/DD/YYYY
 - Time:
 - Default: Null
 - Valid time between 12:00 a.m to 11:59 p.m.
 - Paid vs. Unpaid
 - Default: Null
 - 0-10 characters:
 - Numbers: 0-9

Pre-Conditions:

1. The user is authenticated.
1. The authenticated user is viewing the Bingo Board.
2. The authenticated user clicks on the “Create New Post” button on the top of the page.

Success Outcomes:

1. The post from the authenticated user is uploaded successfully and is displayed on the Bingo Board for other users to view.
2. The post is uploaded to the persistent data store within 3 seconds
3. The authenticated user receives a message indicating successful upload.
4. An info level operational log is created with a message indicating a successful post save in the data store by the authenticated user.
 - a. Level: Info
 - b. Category: Data Store

- c. Message: Bingo Board - BB-1: Post saved successfully.

Failure Outcomes:

1. The post is not stored successfully in the data store or takes longer than 3 seconds to be saved
 - a. Level: Info
 - b. Category: Business
 - c. Message: Bingo Board - BB-1: Operation timeout.
2. If invalid symbol(s) are detected, the post will not be saved and the user will be told to remove the symbol(s).
 - a. Level: Warning
 - b. Category: Business
 - c. Message: Bingo Board - BB-1: Invalid symbols used.

BB - 2: As an authenticated user, I can view my posts on the bingo board and view a list of the registered users who indicated interest.

Complexity Level:

- Low
- Effort points: 6

App Permissions:

- Permission: Read
- Scope: View own posts

Target Audience:

- Authenticated talent or admin users who want to review their postings or view replies to their postings.

Required Inputs:

- N/A

Pre-Conditions:

1. The authenticated user is viewing either the Bingo Board or their profile
 - a. The authenticated user will see an option on both the board or their profile to “View my posts.”

Success Outcomes:

1. The authenticated user is shown a list of posts they have made to the Bingo Board.
 - a. If they have made no posts, will instead display a blank menu saying “No posts made.”
2. Each post shown can be expanded to show the users who have responded.
3. A successful view log is created.
 - a. Level: Info
 - b. Category: View
 - c. Message: Bingo Board - BB-2: Successful display of Bingo Board.

Failure Outcomes:

1. The app takes longer than 3 seconds to display the list of posts or users.
 - a. An operation time log will be created.
2. If the post or reviews fail to load due to a database or technical error, the error will be logged by the system, including timestamp and details of the error. The authenticated user will be notified of the error.
3. An unsuccessful view log is created.
 - a. Level: Error
 - b. Category: View
 - c. Message: Bingo Board - BB-2: Unsuccessful display of Bingo Board.

BB - 3: As an authorized user, I can view the bingo board and see posts made by other users.

Complexity Level:

- Medium
- Effort points: 12

App Permissions:

- Permission: Read
- Scope: View posts

Target Audience:

- Authenticated talent or admin users who want to view gigs and postings in their area or online.

Required Inputs:

- N/A

Optional Inputs:

- Filter settings:

- Authenticated users can adjust whether posts are displayed ordered by:
 - Name of gig
 - Date scheduled for
 - Date posted
- Authenticated users can selectively view posts that are:
 - Local or Online
 - Paid or Unpaid
- Users can expand their search range to show posts from nearby ZIP codes or cities.

Pre-Conditions:

1. An authenticated user navigates to the Bingo Board option from the main menu and clicks on it.
2. If the authenticated user wishes to view more posts, they can click “load more” to load an additional 25 posts.

Success Outcomes:

1. The authenticated user is taken to the Bingo Board and the 25 most relevant posts for their current search settings made by other authenticated users are loaded and displayed.
2. By default, this is the 25 most recent posts.
3. A successful view log is created.
 - a. Level: Info
 - b. Category: View
 - c. Message: Bingo Board - BB-3: Successful display of Bingo Board.

Failure Outcomes:

1. The app takes longer than 3 seconds to load and display posts.
 - a. Level: Error
 - b. Category: Business
 - c. Message: Bingo Board - BB-3: Operation took longer than 3 seconds.
2. If the Bingo Board fails to load posts due to a database or technical error, the error will be logged by the system, including timestamp and details of the error. The authenticated user will be notified of the error.
 - a. Level: Error
 - b. Category: Data Store
 - c. Message: Bingo Board - BB- 3: Bingo Board was unable to access data store.

BB - 4: As an authenticated user, I can view a specific post on the board to see its details and can click a button indicating my interest to the user who posted it.

Complexity Level:

- Low
- Effort points: 6

App Permissions:

- Permission: Read-Write
- Scope: View posts

Target Audience:

- Authenticated admin and talent users viewing the Bingo Board who want to apply for gigs or browse post details.

Required Inputs:

- Clicking on a specific post on the Bingo Board to bring up its details.

Optional Inputs:

- While viewing a post, there will be a button under the details the authenticated user can click to indicate interest.

Pre-Conditions:

1. The authenticated user is viewing the Bingo Board.
2. The authenticated user clicks on a specific post while viewing the Bingo Board

Success Outcomes:

1. When a post is clicked, the correct information is displayed to the authenticated user within 3 seconds.
 - a. Level: Info
 - b. Category: View
 - c. Message: Bingo Board - BB- 4: Bingo Board Post viewed successfully.
2. If they click the interest button, they will be logged and displayed to the poster.

Failure Outcomes:

1. The app takes longer than 3 seconds to load the post.
 - a. Level: Error
 - b. Category: Business
 - c. Message: Bingo Board - BB- 4: Post did not display in 3 seconds.
2. If the post fails to load due to a database or technical error, the error will be logged by the system, including timestamp and details of the error. The authenticated user will be notified of the error.
 - a. Level: Error

- b. Category: Data Store
- c. Message: Bingo Board - BB-4: Bingo Board was unable to access the data store.

BB - 5: As an authenticated user, I can edit or delete a post I have already made.

Complexity Level:

- Low
- Effort points: 6

App Permissions:

- Permission: Read, Edit, Delete
- Scope: Bingo Board posts

Target Audience:

- Authenticated talent or admin users who want to update the details of their posting or delete them entirely.

Required Inputs:

- N/A

Optional Inputs:

- The “Delete” option, if the authenticated user wants to permanently delete the post. If pressed, they will receive a confirmation prompt.

Pre-Conditions:

1. The authenticated user is viewing their own posts through either the Bingo Board or their profile
 - a. The authenticated user will see an option on both the board or their profile to “View my posts.”
2. The authenticated user clicks on the specific post they want to edit/delete.

Success Outcomes:

1. The authenticated user successfully edits and saves their own post, the changes are saved to the persistent data store within 3 seconds.
 - a. Level: Info
 - b. Category: Data Store
 - c. Message: Bingo Board - BB- 5: Post edited successfully.
2. If the authenticated user chooses to delete the post, it is removed from the persistent data store within 3 seconds and other users can no longer view it.

- a. Level: Info
- b. Category: Data Store
- c. Message: Bingo Board - BB- 5: Post deleted successfully.

Failure Outcomes:

1. The app takes longer than 3 seconds to save the changes or delete the post.
 - a. Level: Error
 - b. Category: Business
 - c. Message: Bingo Board - BB- 5: Operation took longer than 3 seconds.
2. If the edit or delete fails due to a database or technical error, the error will be logged by the system, including timestamp and details of the error. The authenticated user will be notified of the error.
 - a. Level: Error
 - b. Category: Data store
 - c. Message: Bingo Board - BB- 5: Bingo Board was unable to access the data store.

Tempo Tool (Metronome):

The tempo tool is a digital metronome to help artists keep time with their music

TT - 1: As an authenticated user, I want to display the metronome feature to keep precise time with my music.

Complexity Level:

- Low
- Effort points: 4

Required Inputs:

- “Enable” option:
 - Displays the metronome
- “Disable” option
 - Hides the metronome

App Permissions:

- Permission: Read
- Scope: Metronome display

Target Audience:

- Any talent role and admin role user that wants to audibly and visually keep time with music.

Pre-Conditions:

1. User must be an authenticated user

Success Outcomes:

1. The metronome is displayed for the authenticated user.
 - a. Log will be recorded according to “View” Default behavior
 - i. Feature: Tempo Tool
 - ii. Feature ID: TT - 1

Failure Outcomes:

1. The Metronome fails to display:
 - a. The authenticated user is presented with an error message that says:
 - i. “Sorry, there was an error displaying the metronome.”
 - b. Log will be recorded according to “Viewing” Default behavior
 - i. Feature: Tempo Tool (Metronome)
 - ii. Feature ID: TT - 1
2. The Metronome fails to be hidden:
 - a. The authenticated user is presented with an error message that says:
 - i. “Sorry, there was an error hiding the metronome.”
 - b. Error is logged for analytics:
 - c. Date and time in UTC format
 - d. Username
 - e. Log Level: Warning
 - f. Log Category: View
 - g. Description
 - i. Feature: Temp Tool
 - ii. User Story ID: TT - 1
 - iii. Log Message: “Metronome failed to be hidden”
3. Displaying or hiding the metronome takes longer than 3 seconds.
 - a. Log will be recorded according to “Operation Time Limits” default behaviors:
 - i. Feature: Temp Tool
 - ii. User Story ID: TT - 1

TT - 2: As a user, I want to adjust the BPM (beats per minute) settings of the metronome for precise tempo control.

Complexity Level:

- Low
- Effort points: 4

Required Inputs:

- Beats Per Minute
 - Integer value ranging from 35 - 250

App Permissions:

- Permission: Write
- Scope: Metronome BPM

Target Audience:

- Any talent role and admin role user who is trying to change the tempo of the metronome.

Pre-Conditions:

1. User must be an authenticated user.
2. Authenticated users must have the metronome actively displayed.

Success Outcomes:

- The authenticated user successfully updates the beats per minute.

Failure Outcomes:

1. Beats per minute fails to update:
 - a. The authenticated user is presented with an error message that says:
 - i. “Sorry, there was an error updating the beats per minute.”
 - b. Error is logged for analytics:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Data
 - v. Description
 1. Feature: Tempo Tool
 2. User Story ID: TT - 2
 3. Log Message: “Beats Per Minute failed to update ”
2. Beats per minute is updated but there is no change in the metronome:
 - a. Error is logged for analytics:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Warning
 - iv. Log Category: Data Store
 - v. Description
 1. Feature: Tempo Tool
 2. User Story ID: TT - 2
 3. Log Message: “Beats Per Minute failed to apply update”
3. Updating the beats per minute takes longer than 3 seconds.
 - a. Log will be recorded according to “Operation Time Limits” default behaviors:
 - i. Feature: Tempo Tool
 - ii. User Story ID: TT - 2

TT - 3: As a user, I want to start and stop the metronome during practice sessions for better control over timing and rhythm.

Complexity Level:

- Low
- Effort points: 4

Required Inputs:

- “Start” option
 - Starts the metronome audio
- “Stop” option
 - stops the metronome audio

App Permissions:

- Permission: Read-Write
- Scope:
 - Metronome Control
 - Metronome Display

Target Audience:

- Any talent role and admin role user that wants to play the audio for the metronome

Pre-Conditions:

1. User must be an authenticated user
2. Authenticated users must have the metronome actively displayed

Success Outcomes:

1. The metronome audio is played for the user.

Failure Outcomes:

1. The metronome audio fails to play:
 - a. The authenticated user is presented with an error message that says:
 - i. “Sorry, there was an error playing the metronome.”
 - b. Error is logged for analytics:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error
 - iv. Log Category: Business
 - v. Description
 1. Feature: Temp Tool
 2. User Story ID: TT - 3
 3. Log Message: “Metronome failed to play”
2. The metronome audio fails to stop play:
 - a. The authenticated user is presented with an error message that says:
 - i. “Sorry, there was an error stopping the metronome.”
 - b. Error is logged for analytics:
 - i. Date and time in UTC format
 - ii. Username
 - iii. Log Level: Error

- iv. Log Category: Business
- v. Description
 - 1. Feature: Temp Tool
 - 2. User Story ID: TT - 3
 - 3. Log Message: “Metronome failed to stop playing”
- 3. Playing or stopping the metronome audio takes longer than 3 seconds.
 - a. Log will be recorded according to “Operation Time Limits” default behaviors:
 - i. Feature: Tempo Tool
 - ii. User Story ID: TT - 3

Scale Display:

Authenticated users will be able to choose a scale and have the notes in that scale displayed on a digital keyboard

SD - 1: As an authenticated user, I want to select a scale type to view notes within that scale.

Complexity Level:

- Low
- Effort Points: 6

App Permissions:

- Permission: View and Read
- Scope: Authenticated users

Target Audience:

- Talent and Admin role users

Required Inputs:

- User authentication credentials (username and password)
- Selection of a specific scale type
 - Major scales
 - Pentatonic scales
 - Lydian scales
 - Dorian scales
 - Minor scales
 - Harmonic minor scales

Pre-Conditions:

1. The authenticated user must be logged in with a valid username and password.
2. The authenticated user is accessing the Scale Display interface.
3. Scale types are available for selection.

Success Outcomes:

1. The authenticated user can access and view all of the following scale types:
 - a. Major scales
 - b. Pentatonic scales
 - c. Lydian scales
 - d. Dorian scales
 - e. Minor scales
 - f. Harmonic minor scales
2. The user can select a specific scale type from the available options.
 - a. Upon selecting a scale type, the system displays the relevant notes within that scale.
3. A log is created after a user has used selected which scale they would like to be displayed:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Info
 - d. Log Category: View
 - e. Description
 - i. Feature: Scale Display
 - ii. User Story ID: SD - 1
 - iii. Log Message: "Displaying [chosen scale]"

Failure Outcomes:

1. Authenticated users are unable to see the list of scales they can choose from
2. After choosing a scale, the user is unable to see the notes associated with the scale
3. A log is created after a user selects a scale, but cannot see notes:
 - a. Date and time in UTC format
 - b. Username
 - c. Log Level: Error
 - d. Log Category: View
 - e. Description
 - i. Feature: Scale Display
 - ii. User Story ID: SD - 1
 - iii. Error Message: "Scale notes could not be displayed"

Glossary:

Business Terms:

- Composer: An artist who makes original music from the ground up
- Arranger: An artist that arranges music that already exists in their own way
- Instrumentalist: Anyone who plays a musical instrument

- Cover artist: An artist who makes a cover of a song that already exists
- Audio Waveform: A graph that displays amplitude or level changes of any audio over time.
- Metronome: A device that produces an audible click/sound at a regular interval that can be set by the user, typically in BPM
- BPM: Beats per minute is a measurement of a song's tempo
- Tempo: The rate of speed at which a musical piece or passage is to be played

Technical Terms:

- Persistent Data Store: a database designed to retain data even when the application or system using it is shut down or restarted.

Resources:

<https://wmich.edu/mus-gened/mus150/Glossary.pdf>

<https://www.soundbridge.io/what-are-waveforms-how-they-work>