**Group 1 Data Management Plan (Iteration 2)**

**Darren Ross**

**Anthony Jack**

**Manikala Chevitipalli**

**Sai Achyuth Konda**

**GitHub Wiki Page:** <https://github.com/djgamekid/GDP-Group-I-bearcatmanager/wiki/Data-Management-Plan-(Iteration-2)>

**Summary of Data to be Stored**

**1. Admin Information**

* Admin ID: A unique identifier for each admin.
* Name: The name of the admin.
* Email: The email address of the admin.
* Role: The role of the admin within the system.

**2. User Information**

* User ID: A unique identifier for each user (student or staff).
* Name: The name of the user.
* Email: The email address of the user.
* Role: The role of the user (either Student or Staff).

**3. Event Details**

* Event ID: A unique identifier for each event.
* Admin ID: The identifier for the admin managing the event.
* Name: The name of the event.
* Description: A brief description of what the event is about.
* Time: The time the event starts.
* Location: Where the event will take place.
* Date: The date the event is scheduled for.

**4. Ticket Information**

* Ticket ID: A unique identifier for each ticket type.
* Admin ID: The identifier for the admin managing the event.
* Event ID: The identifier for the event associated with the ticket.
* Type: The type of ticket (e.g., NOM or VIP).
* Price: The cost of the ticket.
* Availability: The number of tickets available for purchase.

**5. Attendance Records**

* Attendance ID: A unique identifier for each attendance record.
* Event ID: The identifier for the event for which the user is attending.
* User ID: The identifier for the user attending the event.
* Status: The status of the user’s attendance (e.g., checked in or not).

**6. Notification Details**

* Notification ID: A unique identifier for each notification.
* User ID: The identifier for the user receiving the notification.
* Message: The content of the notification message.
* Type: The type of notification (e.g., Email, SMS, or App notification).

**7. Payment Information**

* Payment ID: A unique identifier for each payment transaction.
* User ID: The identifier for the user making the payment.
* Event ID: The identifier for the event associated with the payment.
* Admin ID: The identifier for the admin managing the event.
* Amount: The amount paid.
* Payment Status: The status of the payment (e.g., completed, pending, failed).

**Data Security Plans**

**Initial Plans to Secure Data**

1. **Access Restrictions:**
   1. User Roles: Implement role-based access control (RBAC) to ensure that users only have access to data necessary for their role (e.g., Admin, User, Event Organizer).
      1. Admins will have full access to manage events, users, and notifications.
      2. Users (Students/Staff) will have restricted access, allowing them to view and register for events, purchase tickets, and receive notifications.
   2. Authentication: Require strong authentication methods (e.g., password policies, two-factor authentication) to access the system and sensitive data.
2. **Data Encryption:**
   1. At Rest: Use encryption to secure sensitive data stored in the database, such as user emails, payment information, and notifications. AES (Advanced Encryption Standard) is recommended for this purpose.
   2. In Transit: Implement HTTPS to encrypt data transmitted between users and the server, preventing interception during data exchange.
   3. Sensitive Fields: Specifically encrypt sensitive fields like Email, Payment Amount, and Notification Message to further enhance security.
3. **Regular Security Audits:**
   1. Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks in the system.
4. **Data Backup and Recovery:**
   1. Implement a data backup strategy to ensure that all data is regularly backed up and can be restored in the event of data loss or a security breach.

**Mapping of Functional Requirements to Data Storage**

1. **User Registration and Management:**
   1. Related Data Storage: User table
   2. Requirements: Store user information securely and allow admins to manage user accounts.
2. **Event Management:**
   1. Related Data Storage: Event table, Admin table
   2. Requirements: Admins need to create, update, and delete events, associating them with their profiles.
3. **Ticket Sales:**
   1. Related Data Storage: Ticket table, Payment table
   2. Requirements: Users should be able to purchase tickets, and relevant payment data should be securely stored and processed.
4. **Attendance Tracking:**
   1. Related Data Storage: Attendance table
   2. Requirements: Track user attendance at events, enabling event organizers to manage participants effectively.
5. **Notifications:**
   1. Related Data Storage: Notification table
   2. Requirements: Notify users about events, updates, and reminders securely without exposing sensitive information.
6. **Payment Processing:**
   1. Related Data Storage: Payment table
   2. Requirements: Securely store transaction details, including user IDs and event IDs, to track payments made by users