6. Other Requirements

6.1. Legal and Compliance Requirements:

6.1.1. Data Protection and Privacy:

- The Smart Attendance System (SAS) must comply with relevant data protection laws, including but not limited to GDPR, ensuring the privacy and security of user data.
- The system should provide mechanisms for obtaining user consent for data processing and clearly communicate the purposes of data collection.

6.2. Performance Requirements:

6.2.1. Response Time:

- The system should respond to user interactions, such as attendance recording and report generation, within an acceptable time frame. Response times should not exceed 2 seconds for common operations.

6.2.2. Scalability:

- The SAS should be designed to handle a scalable number of users, classes, and attendance records. Performance testing should be conducted to ensure the system's responsiveness as the user base grows.

6.3. Security Requirements:

6.3.1. User Authentication:

- The system must implement secure user authentication mechanisms, including password protection and, if applicable, two-factor authentication, to prevent unauthorized access.

6.3.2. Data Encryption:

- All sensitive data, including user credentials and attendance records, must be encrypted during transmission and storage to prevent unauthorized access.

6.4. User Training and Support:

6.4.1. Training Material:

- The development team should provide comprehensive training materials, including user manuals and video tutorials, to facilitate user onboarding and system understanding.

6.4.2. Help Desk Support:

- A help desk or customer support system should be established to assist users with inquiries, issues, or technical difficulties related to the Smart Attendance System.

6.5. System Maintenance and Updates:

6.5.1. Maintenance Schedule:

- A regular maintenance schedule should be established to address system updates, bug fixes, and any necessary improvements. Maintenance activities should be communicated to users in advance.