Table of Contents

[System Components and Design 1](#_Toc178839505)

[Purpose 1](#_Toc178839506)

[System Background 2](#_Toc178839507)

[Objectives and Goals 3](#_Toc178839510)

[Requirements 4](#_Toc178839512)

[Nonfunctional Requirements 4](#_Toc178839513)

[Functional Requirements 8](#_Toc178839514)

[User Interface 9](#_Toc178839515)

[Assumptions 10](#_Toc178839516)

[Limitations 11](#_Toc178839517)

[Gantt Chart 12](#_Toc178839518)

# System Components and Design

## Purpose

The DriverPass system is designed to offer a comprehensive application that helps individuals prepare for their driving tests and ultimately obtain their driver’s license. The application provides multiple user-centered functions to ensure users are well-prepared before their official testing.

**Client:**

* **Company**: DriverPass
* **Key Stakeholders**:
  + **Liam**: Owner
  + **Ian**: IT Officer

**Core Functions:**

* **Practice Online Driving Tests**:
  + Users can take practice driving tests to prepare for the official exam, simulating real-world questions and scenarios.
* **Schedule In-Person Driving Tests**:
  + Users can book in-person driving tests with company-provided instructors through the system’s scheduling feature.
* **Review Instructor Notes**:
  + After each driving lesson, users can access and review their instructor’s feedback and notes within the application to track their progress and areas for improvement.
* **Select Training Packages**:
  + Users can browse and choose from different training packages tailored to their needs.
* **View and Edit Training Appointments**:
  + Users have the ability to view, modify, or cancel their scheduled training sessions through the application, providing flexibility in managing their appointments.

This system aims to streamline the driving test preparation process, offering a user-friendly and supportive environment to ensure users are fully prepared before their driving test.

## System Background

Based on the client's needs and interview feedback, the system must include the following components and features:

**Cloud Infrastructure:**

* The system will be cloud-based, offering:
  + **Data Storage**: All user and system data will be securely stored in the cloud.
  + **Backups**: Automatic backups to ensure data is preserved and recoverable.
  + **Security**: Cloud security features must include encryption, access control, and regular vulnerability assessments.

Cross-Platform Accessibility:

* The system will be accessible from desktop and mobile platforms, ensuring users can interact with the system from various devices.

External Integration:

* The system must have a direct connection to the **DMV system**, allowing secure data exchange and integration with relevant DMV services.

**Web-Based User Interface:**

* The system’s user interface will be web-based, ensuring:
  + **Ease of Access**: Users can access the system via standard web browsers without additional software.
  + **User-Friendly Design**: The interface will be intuitive and designed for ease of use, regardless of the user's technical expertise.

These components will ensure the system meets the client's requirements for accessibility, functionality, and security while also supporting external integrations and platform flexibility.

## Objectives and Goals

At the conclusion of the project, the system must provide the following features and functionalities:

**User Interface:**

A smooth, intuitive interface allowing easy navigation between pages, with the following capabilities:

* + **Page Navigation**:
    - View and manage business contact information.
    - Edit user information.
    - Access appointments.
    - Online tests.
  + **View Progress**:
    - Track progress on online tests.
  + **Test Functionality**:
    - Take online tests within the system.
  + **Training Package Selection**:
    - Choose and register for a training package.
  + **Appointment Management**:
    - Schedule and edit appointments.
    - Set pickup/drop-off locations for appointments.

Export Functions:

Provide downloadable reports for offline use.

* **Administrative Functions**:
  + Allow users to reset passwords.
  + Implement role-based access control, separating functionality for:
    - Admins.
    - Company personnel.
    - Average users.
* **Historic Tracking**:
  + Track and store system changes by user, including:
    - Appointment modifications.
    - Activity reports for system interactions.

# Requirements

## Nonfunctional Requirements

**Performance Requirements**

* **Platform Compatibility**:  
  The system must run seamlessly across all major web browsers, including:
  + Chrome
  + Edge
  + Firefox
  + Safari
* **System Speed**:  
  The system's performance should adapt to the user’s internet connection, ensuring it responds in real-time with minimal latency under standard broadband conditions.
* **Backup and Maintenance Schedule**:
  + **Nightly Partial Backups**: Incremental backups should occur nightly to preserve daily changes and ensure minimal data loss.
  + **Weekly Full Backups**: The system will conduct full backups weekly to maintain comprehensive data integrity and restore capabilities in case of system failure.

These performance requirements ensure that the DriverPass system remains fast, reliable, and compatible across different platforms while safeguarding user data through regular backups.

**Platform Constraints**

* **Supported Platforms**: The DriverPass system will be web-based and must be accessible from any platform with a web browser, including:
  + **Windows** (via browsers such as Chrome, Edge, Firefox)
  + **macOS** (via Safari, Chrome, Firefox)
  + **Linux/Unix** (via Chrome, Firefox)
  + **Mobile Devices** (iOS and Android) using responsive web design for compatibility with mobile browsers (e.g., Safari, Chrome)
* **Back-End Requirements**: The system’s back end will require the following tools to support the application:
  + **Cloud Infrastructure**:
    - A cloud platform (e.g., **AWS**, **Google Cloud**, or **Azure**) to manage data storage, backups, and security, providing scalable infrastructure for the system.
  + **Web Server**:
    - A web server (e.g., **Apache** or **Nginx**) to handle HTTP requests and ensure smooth communication between the client and server.
  + **API Integrations**:
    - The system will need API integrations, particularly to connect with external systems such as the **DMV** for scheduling and test-related data sharing.

These platform constraints ensure that the system is accessible from various operating systems and devices while utilizing the necessary backend tools to provide scalability, reliability, and security.

**Accuracy and Precision**

* **User Identification**:
  + **Unique User Accounts**: Each user will be identified by a unique email address and password combination. This ensures that every user is distinct, and multiple accounts with the same email address are not allowed.
  + **Role-Based Access**: The system will distinguish between user roles (e.g., **admin**, **instructor**, **student**), each having different levels of access and functionality within the system.
* **Input Sensitivity**:
  + **Case Sensitivity**:
    - **Passwords**: Passwords will be case-sensitive to ensure higher security.
    - **Username/Email**: Email addresses will not be case-sensitive, allowing users to log in regardless of the case used when typing their email.
    - **Forms and Input Fields**: Input fields, such as names and addresses, will be case-insensitive for consistency, except where security or specific formatting is required (e.g., passwords).
* **System Alerts for Admin**:
  + **Error Reporting**: The system should notify the admin when critical issues occur, such as:
    - **System Failures**: If a critical system function, like backup or user authentication, fails.
    - **Data Integrity Issues**: In case of database corruption or failed backups.
    - **Security Breaches**: If there is unauthorized access or a failed login attempt threshold is reached (e.g., more than five failed login attempts in a short time).
  + **Regular Monitoring**: Automated logs and monitoring tools should be in place to track system performance, with notifications sent to the admin when resource usage (e.g., CPU, memory) exceeds a predefined threshold.

These accuracy and precision measures ensure the system operates reliably, securely distinguishes between users, and proactively alerts admins to potential issues before they escalate.

**Adaptability**

* **User Management (Add/Remove/Modify Without Code Changes)**:
  + **Admin Dashboard for User Management**:
    - The system will include an admin dashboard that allows administrators to easily add, remove, or modify user accounts, roles, and permissions through the web interface without changing the underlying code.
    - **Role-Based Access Control (RBAC)**: Admins can assign or modify roles (e.g., student, instructor, admin) and update user information dynamically via the system interface.
  + **Self-Service**: Users can modify their profiles (e.g., change password, update contact information) within the platform without IT or admin intervention.
* **Adaptation to Platform Updates**:
  + **Cross-Browser Compatibility Testing**: The system will undergo regular testing across major browsers (Chrome, Firefox, Safari, Edge) to ensure compatibility after platform updates.
  + **Responsive Design**: The user interface will use responsive design principles to ensure it adapts smoothly to changes in device or browser updates, ensuring consistent functionality across platforms.
  + **Cloud-Based Hosting**: Since the system is cloud-based, platform updates (e.g., new browser versions or OS changes) will be managed centrally, reducing the need for system-wide updates. This provides flexibility to adapt to changes without significant disruptions.
* **IT Admin Access**:
  + **Full Administrative Access**: The IT admin will have full administrative rights to:
    - **Manage Users**: Add, remove, or modify user accounts, roles, and permissions.
    - **System Monitoring**: Access logs, system health reports, and security settings to monitor system performance and address issues as they arise.
    - **Backup and Restore**: Initiate backups, restore data from backups, and manage data retention settings.
    - **Security Settings**: Configure security protocols and respond to security incidents.

These features ensure the system is adaptable to user management needs and platform changes while granting IT admins the necessary access to maintain and secure it.

**Security**

* **User Login Requirements**:
  + **Username or Email**: Users must provide their registered username or email address.
  + **Password**: Users must enter their password, which should be case-sensitive for enhanced security.
* **Securing the Connection and Data Exchange**:
  + **Use of HTTPS**: The system must implement HTTPS (Hypertext Transfer Protocol Secure) to encrypt data transmitted between the client and server, ensuring that sensitive information (like login credentials and personal data) is protected during transmission.
  + **TLS Encryption**: Employ Transport Layer Security (TLS) to secure data exchanges, preventing interception and tampering.
  + **Input Validation and Sanitization**: Ensure all user inputs are validated and sanitized to prevent SQL injection and other attacks.
* **Account Handling During Brute Force Attempts**:
  + **Account Lockout Mechanism**:
    - **Failed Login Attempts**: After a predefined number of failed login attempts (e.g., five attempts), the system will temporarily lock the user’s account for a specific duration (e.g., 15 minutes).
    - **Email Notification**: Notify the user via email if their account has been locked due to suspicious activity, providing instructions on unlocking it.
  + **Admin Alerts**: The system should automatically alert the IT admin about repeated failed login attempts from the same IP address, allowing for monitoring and investigation of potential security threats.
* **Password Recovery Process**:
  + **Forgot Password Option**:
    - **Password Reset Request**: Users can initiate a password reset by clicking on a "Forgot Password?" link on the login page and entering their registered email address.
    - **Email Verification**: The system will send a secure password reset link to the registered email. This link should expire after a short period (e.g., 1 hour) to enhance security.
  + **Password Reset**:
    - Upon clicking the reset link, users will be directed to a secure page to enter a new password. The new password must meet defined complexity requirements (e.g., a mix of uppercase letters, lowercase letters, numbers, and special characters).

By implementing these security measures, the DriverPass system can ensure secure user authentication, protect against unauthorized access, and provide a user-friendly experience for password recovery while safeguarding user data.

## Functional Requirements

**User Authentication:**

* The system shall validate user credentials when logging in.
* The system shall provide an option for users to reset their passwords if they forget them.

**User Management:**

* The system shall allow administrators to add, modify, or remove user accounts.
* The system shall enable users to update their personal information, including email and password.

**Driving Test Preparation:**

* The system shall provide online practice driving tests for users to simulate actual test scenarios.
* The system shall allow users to select and register for different training packages based on their needs.

**Appointment Scheduling:**

* The system shall enable users to schedule in-person driving tests with company-provided instructors.
* The system shall allow users to view and edit their training appointments.
* The system shall permit users to set pickup/drop-off locations for driving appointments.

**Instructor Interaction:**

* The system shall allow users to review their instructor’s notes and feedback after each lesson.
* The system shall notify users of any scheduled appointments or instructor availability changes.

**Data Management:**

* The system shall store user data securely, including test results, personal information, and appointment history.
* The system shall conduct nightly partial backups and weekly full backups of all user data to ensure data integrity.

**Reporting and Analytics:**

* The system shall generate reports for administrators on user progress, test performance, and appointment histories.
* The system shall allow users to view their real-time test progress and performance metrics.

**Security Measures:**

* The system shall log all successful and unsuccessful login attempts to monitor for suspicious activity.
* The system shall notify the user and the admin in the event of a brute force attack or multiple failed login attempts.

These functional requirements provide a comprehensive overview of the capabilities and features the DriverPass system must deliver to ensure a smooth and efficient user experience while maintaining security and data integrity.

## User Interface

**User Needs of the Interface:**

* **Intuitive Design**: The interface must be user-friendly and intuitive, allowing users to navigate seamlessly without requiring extensive training.
* **Responsive Layout**: The design should adapt to various screen sizes and orientations, ensuring usability on desktops, tablets, and mobile devices.
* **Consistent Navigation**: Navigation elements should be consistent throughout the application, providing users with familiar and predictable pathways.

**User Needs and Capabilities:**

* **Students**:
  + **Log In**: Access their accounts using credentials.
  + **Practice Tests**: Take online driving practice tests and receive immediate feedback.
  + **Schedule Appointments**: Schedule, view, and edit their driving lessons and in-person tests.
  + **Review Notes**: Access feedback and notes from their instructors.
  + **Select Training Packages**: Choose from different training packages based on their preferences.
* **Instructors**:
  + **Log In**: Access their accounts to manage student information.
  + **View Student Progress**: Check the progress and performance of their students.
  + **Provide Feedback**: Enter notes and feedback after lessons for students to review.
  + **Manage Schedule**: View and manage their own schedules and appointment slots.
* **Administrators**:
  + **Log In**: Access the admin dashboard with elevated privileges.
  + **User Management**: Add, modify, or delete user accounts as needed.
  + **Data Reports**: Generate and view reports on user activities, test performances, and system usage.
  + **System Monitoring**: Monitor system health, performance, and security alerts.

**User Interaction with the Interface:**

* **Desktop Browsers**: Users will access the system via major web browsers (Chrome, Firefox, Safari, Edge), providing a full-featured experience.
* **Mobile Devices**: The system will have a responsive design that allows users to access it through mobile browsers, ensuring functionality on smartphones and tablets.
* **Touch and Mouse Interaction**: The interface should support touch gestures (for mobile users) and mouse interactions (for desktop users) for easy navigation.
* **Notifications**: Users will receive notifications (e.g., appointment reminders and instructor feedback) through the interface, enhancing engagement and communication.

By addressing these interface needs, the DriverPass system will provide a comprehensive, user-friendly platform that meets its users' diverse requirements while ensuring accessibility and ease of use.

## Assumptions

**User Familiarity with Technology:**

* It is assumed that users (students, instructors, and administrators) have a basic understanding of how to navigate web applications and mobile interfaces.
* Users are expected to be comfortable using email for account verification and password recovery.

**Internet Connectivity:**

* The design assumes that users will have reliable internet access to use the application effectively on mobile or desktop devices.
* The system's performance is assumed to be optimal on standard broadband connections and may be affected by slower internet speeds.

**Device Compatibility:**

* It is assumed that users will access the system on modern devices (smartphones, tablets, laptops, and desktops) capable of running current versions of major web browsers.

**Security Measures:**

* It is assumed that users will adhere to best practices for account security, such as choosing strong passwords and keeping their login credentials confidential.

Acknowledging these assumptions allows the design to be further refined to address potential gaps and ensure that the DriverPass system effectively meets the needs of all users.

## Limitations

**Technical Limitations:**

* **Browser Compatibility**: While the system aims to be compatible with major web browsers, variations in how browsers render content may lead to inconsistencies in user experience.
* **Mobile Device Variability**: The design may not fully account for the wide range of mobile devices with differing screen sizes, operating systems, and capabilities, potentially impacting functionality and usability.

**Performance Constraints:**

* **Server Load**: The system’s performance may degrade under high user loads, especially during peak usage times (e.g., before driving tests), unless adequate server resources are provisioned.
* **Data Processing Speed**: Generating real-time reports and analytics may slow down if the volume of data is large, potentially leading to delays in user experience.

**User Behavior:**

* **Assumption of Compliance**: The design assumes users will follow security best practices, such as not sharing passwords. Non-compliance could expose the system to security vulnerabilities.
* **Variability in User Proficiency**: Despite efforts to make the interface user-friendly, users with varying levels of technical proficiency may find it challenging to navigate the interface.

**Resource Limitations:**

* **Time Constraints**: The development timeline may limit the ability to conduct extensive user testing or iterative improvements, potentially resulting in undiscovered usability issues.
* **Budget Constraints**: Budget limitations may restrict the ability to implement advanced features (e.g., sophisticated analytics, personalized user experiences) or hire specialized personnel for design and development.

**Integration Challenges:**

* **Third-Party System Integration**: Compatibility issues may limit the system’s ability to connect with external organizations, like the DMV.

**Feature Scope:**

* + **Scalability Issues**: As the user base grows, scaling the system to accommodate additional features or user load may require significant further investment in infrastructure.

**Support and Maintenance:**

* + **Ongoing Maintenance Needs**: The system will require ongoing maintenance and updates, which could strain resources if not adequately planned for in the project scope.
  + **User Support**: Providing sufficient user support (e.g., help desk, tutorials) may be limited due to budget and resource constraints, affecting user satisfaction and engagement.

By recognizing these limitations, stakeholders can better prepare for potential challenges and develop strategies to mitigate risks associated with the DriverPass system.

## Gantt Chart

