Slide 1



Slide 2



**Functional Requirements**

- The system allows end users to choose one from the existing packages and grant access to the learning course while identifying different users by their permissions.

- The system allows end users to book/cancel/modify their appointments, view their progress, read the instructor's feedback, and manage their accounts.

**Nonfunctional Requirements**

- The system is responsive, supported by any digital device, and delivered as a web-based, 24/7 app from any internet-connected device.

- The system will support the highest security encryption standards to prevent breaches and data loss to ensure safe usage.

Slide 3



As requested, the system is scalable and supports fast multiuser access.

It grants full system access to the user admin and limited access to the company secretary role. At the same time, the instructors can update and manage students' technical progress, while the secretary and the admin can handle the operational aspect of the business by updating their packages and classes and taking care of the financial and administrative perspectives.

In addition, the system is connected to the main DMV offices to pull updates and new driving regulations.

Your client is the main system user who can manage his account, enroll in different classes, schedule and update his driving lessons, and benefit from comprehensive feedback from the instructor.

Slide 4



The above example provides a breakdown of the lesson reservation process and how your client is performing it.

After a successful login, the system recognizes the user as a student and reads his data from the database.

Next, it verifies the attached instructor's schedule and provides the student with available dates and times to book his next lesson.

As a timeslot has been picked, the system updates the instructor's calendar while preventing multiplicity and scheduling errors.

As the appointment is confirmed, it notifies the client and updates the management of a new or modified reservation as requested by DriverPass.

Slide 5



The app will comply with relevant data protection regulations and standards, including encryption and secure authentication mechanisms.

Each registered user will log in with their chosen email address and a unique password containing a minimum of 8 characters, letters, numbers, and symbols. The app's robust two-step authentication mechanism, used during the initial registration process or password recovery, ensures the user’s identity is verified with confidence.

The communication between the app’s back and front end is secured with SSL/TLS protocols, while the passwords and sensitive data are encrypted with the SHA-256 algorithm. To prevent brute force attacks user's account will lock down after three incorrect password inputs while providing users or the staff to recover forgotten passwords.

Slide 6



The system's proper operation depends on several factors and limitations, such as limited functionality once the internet or connection to the server is lost and/or not accessible during the monthly downtime update sessions.

In addition, the system assumes that user devices will meet or exceed minimum system requirements and that their security protocols will be up to date. Nonetheless, the accuracy of the regulations provided by the app is directly related to the DMV's API connectivity.