# CS 255 System Design Document Template

This template lays out all the different sections that you need to complete for Project Two. Each section has guidance to prompt your thinking. You will need to continually reference the interview transcript as you work to make sure that you are addressing your client’s needs. There is no required length for the final document. Instead the goal is to complete each section based on what your client’s needs are. Remove this note when you are finished, and replace all bracketed text with the relevant information.

## UML Diagrams

### A screenshot of a cell phone AI-generated content may be incorrect.UML Use Case Diagram

### UML Activity Diagrams

A screenshot of a computer

AI-generated content may be incorrect.

A diagram of a flowchart

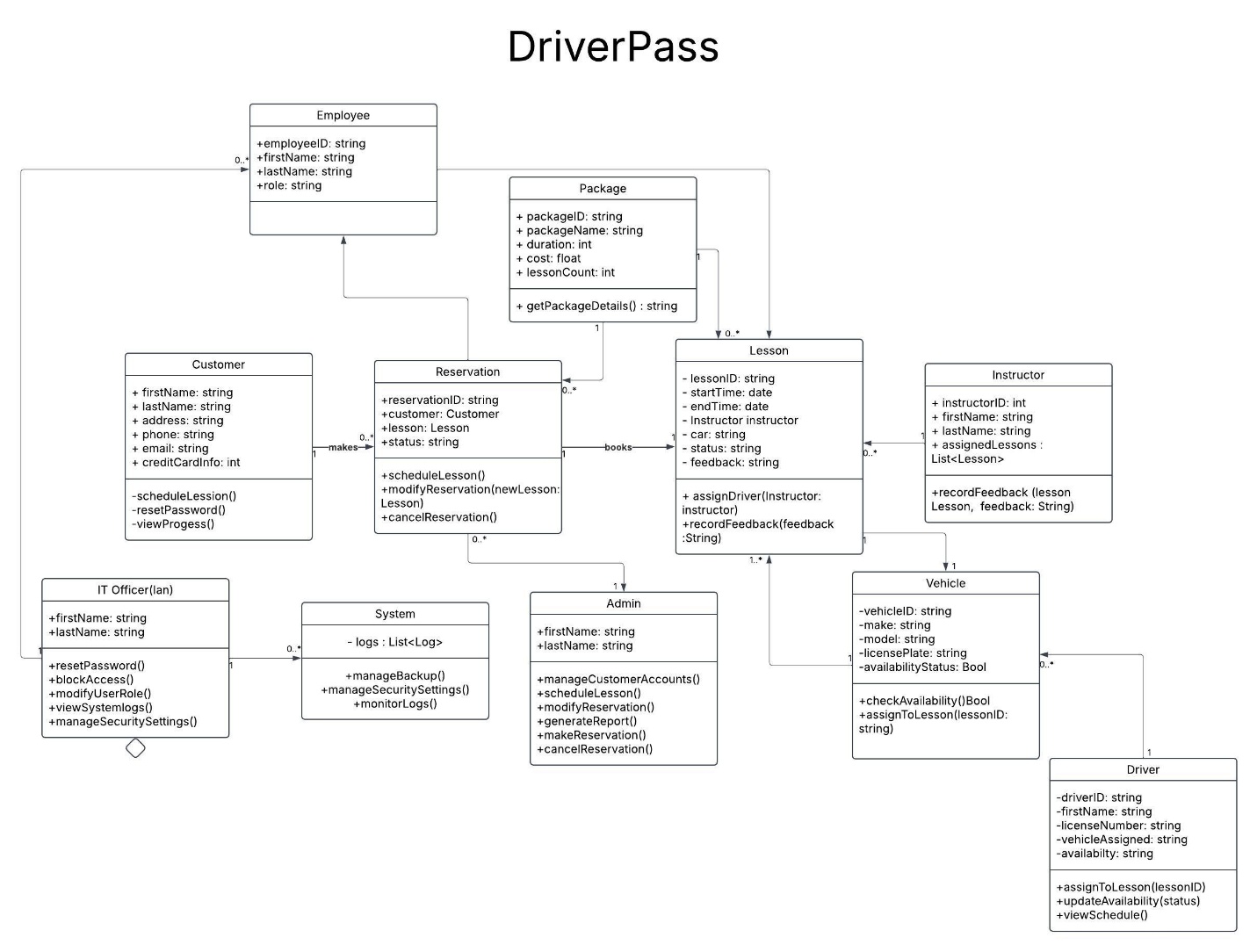
AI-generated content may be incorrect.

### UML Sequence Diagram

A diagram with blue squares

AI-generated content may be incorrect.

### UML Class Diagram



## Technical Requirements

The DriverPass system will be a web-based platform designed for accessibility across all major web browsers and mobile devices. It will require a robust backend infrastructure to ensure seamless operation and high performance. The system's core will be built using a reliable framework such as Django or Node.js, providing scalability and maintainability. The front-end will leverage React for an intuitive user experience and responsive design, ensuring compatibility with various screen sizes.

A relational database, such as MySQL, will be implemented to store critical user data, including customer accounts, test results, lesson schedules, and payment details. Cloud hosting services will be utilized to ensure scalability and reliability, enabling the system to handle up to 1,000 concurrent users without performance degradation. Load balancing and caching mechanisms will be employed to optimize performance and reduce latency.

Security will be a top priority, with HTTPS encryption ensuring secure communication between clients and the server. User authentication will be managed using industry-standard authentication protocols, including multi-factor authentication (MFA) where necessary. Sensitive data, such as payment information, will be encrypted using secure cryptographic methods to protect against data breaches.

The system will support role-based access control, allowing different user types (customers, instructors, admins, IT officers) to have appropriate permissions and restrictions. Automated backups and disaster recovery measures will be in place to safeguard data integrity. Additionally, the system will be designed to adapt to future platform updates and regulatory changes, ensuring long-term sustainability and compliance with evolving industry standards.

Regular system updates, occurring every 3-6 months, will address security patches, performance enhancements, and feature improvements. Continuous monitoring and logging will be implemented to detect and prevent potential threats, ensuring a secure and stable environment for all users.