# CS 255 System Design Document Template

## UML Diagrams

### UML Use Case Diagram



### UML Activity Diagrams





### UML Sequence Diagram

**

### UML Class Diagram

**

## Technical Requirements

The DriverPass system requires a solid combination of hardware, software, tools, and infrastructure to operate efficiently and securely. For hardware, the system should be hosted on a reliable server with at least an 8-core CPU and 32 GB of RAM to manage backend processes like user authentication, appointment scheduling, and online testing. A separate database server with higher storage capacity and redundancy (e.g., RAID setup) is recommended to ensure consistent performance and data safety. Client access can be achieved through standard computers, tablets, or smartphones with modern web browsers, while backup solutions must be in place for nightly data storage and recovery.

On the software side, the server should run a stable operating system such as Ubuntu Server 22.04 LTS or Windows Server 2022. A web server like Apache or Nginx will manage HTTP requests, while the database can be powered by MySQL 8.0 or PostgreSQL 15 to handle user profiles, appointments, tests, and results data. Backend services should be developed using languages like Java, or Python, supporting modern frontend frameworks such as ReactJS or Angular for a responsive user interface. To secure login sessions (as shown in the sequence diagram), authentication frameworks such as OAuth 2.0 and JWT (JSON Web Tokens) must be implemented. Testing frameworks like Selenium and Postman are needed to ensure system quality across different components.

In terms of development tools, integrated development environments (IDEs) like Visual Studio Code, or Eclipse will facilitate coding and debugging. Version control must be handled with Git, hosted on platforms such as GitHub or GitLab, while Jenkins or GitHub Actions should be used for continuous integration and deployment (CI/CD). Containerization tools like Docker can also be beneficial for modular and scalable deployments, especially if cloud hosting is considered. Monitoring tools such as Prometheus and Grafana will be necessary to oversee server performance and detect issues early.

Finally, the infrastructure must support secure, scalable operations. A registered domain name and SSL/TLS certificates will ensure encrypted communications. If scalability is a concern, the system should leverage cloud hosting services like AWS, Azure, or Google Cloud, with load balancers to distribute user traffic efficiently. Firewalls and intrusion prevention systems must be part of the deployment to safeguard against cyber threats, ensuring the system’s integrity while serving the DriverPass Center, Students, and DMV interfaces effectively.