Case study

As an initiative towards the ‘Green Campus’ for minimising the carbon footprint, traffic congestion, and noise pollution by vehicles, the University’s administration has decided to provide a bicycling service to the campus visitors. The visitors can rent the available bike(s) on an hourly or daily basis to enhance in-campus mobility by using the CampusBike mobile application. The By using the application, campus visitors as potential bikers can register with the CampusBike system to view available bikes, e.g., location proximity < 500 meters to reserve the bike for a specific time interval, e.g., 60 minutes. To support this scenario, the university administration needs to develop a software application CampusBike that operates in a networked environment by enabling the users to register with the system, view available bikes, reserve and return a bike and make payments for the ride. The data of the visitors, i.e., bike riders must be managed securely and preserve privacy as per the GDPR regulation.

Based on the given scenario, the security requirements for the CampusBike system can include:

1. User Authentication: Implement a secure authentication mechanism to verify the identity of users during registration and login processes.

2. Data Encryption: Apply encryption techniques to protect sensitive data, such as user credentials, payment details, and personal information stored in the system's database.

3. Access Control: Enforce access control measures to ensure that only authorized individuals have appropriate privileges to view, modify, or delete user and bike-related data.

4. Secure Communication: Utilize secure protocols (e.g., HTTPS) for transmitting data between the system and users' devices to prevent unauthorized interception or tampering of sensitive information.

5. Secure Payment Processing: Implement secure payment gateways and comply with industry-standard security practices to protect users' payment information during payment processing.

6. GDPR Compliance: Adhere to the GDPR regulations regarding the collection, storage, and processing of personal data, ensuring user privacy and obtaining appropriate consent from users.

7. Regular Security Audits: Conduct periodic security audits and vulnerability assessments to identify and mitigate any potential security risks or vulnerabilities in the system.

8. Secure Backup and Recovery: Implement regular data backups and secure recovery processes to prevent data loss and ensure system availability in the event of any unforeseen incidents or system failures.

9. User Privacy Protection: Implement privacy controls and measures to protect users' personal information, including appropriate data anonymization, pseudonymization, and data minimization techniques.

10. Incident Response and Reporting: Establish an incident response plan to promptly address and mitigate security incidents, as well as mechanisms for reporting and handling any security breaches or data breaches in accordance with legal requirements.

It is important to note that the specific security requirements may vary depending on the system architecture, infrastructure, and any additional legal or regulatory obligations applicable to the University.