3.6 Inverse Requirements

1. No Guest Checkout

User-Side: Users must register and log in before proceeding to purchase, ensuring a secure and trackable shopping experience.

System-Side: The system enforces login before checkout, disabling guest checkout options and maintaining session consistency for order tracking and support.

2. No Unsecured Payment Processing

User-Side: Users will complete payments only through secure, integrated gateways to ensure protection of financial data.

System-Side: All payment processing is routed through PCI DSS-compliant, integrated payment gateways, blocking external or insecure payment methods.

3. No Unauthorized Access to Admin Features

User-Side: Only authenticated administrators have access to administrative features like order management, inventory, and reports.

System-Side: Role-based permissions restrict access to sensitive admin functions, preventing unauthorized users from accessing management features.

4. No User-to-User Communication

User-Side: Users cannot interact or communicate directly with one another, ensuring privacy and reducing potential conflicts.

System-Side: The platform lacks direct messaging or communication channels between users, enforcing a policy of privacy and security.

5. No Modification of Critical Data by Users

User-Side: Users cannot alter historical order details or transaction records after completion, maintaining data accuracy.

System-Side: Critical data is protected against user modifications post-transaction, ensuring data integrity and compliance.

---

3.7 Design Constraints

1. Security Compliance

User-Side: Users’ personal and financial data are securely stored and handled, complying with GDPR and PCI DSS regulations.

System-Side: The system stores all personal data in encrypted formats, using secure hashing for passwords and ensuring compliance with relevant standards.

2. Mobile Compatibility

User-Side: The platform provides a responsive and optimized experience on mobile devices, ensuring functionality across devices.

System-Side: The user interface is designed to adapt to various screen sizes and mobile devices, enhancing accessibility and usability.

3. Hosting Environment

User-Side: Users experience stable performance even during peak times due to the scalable cloud-based infrastructure.

System-Side: The platform is hosted on a scalable cloud service (e.g., AWS, Azure) to accommodate traffic spikes and maintain performance.

4. API Integration Standards

User-Side: Users benefit from integrated features like payment processing, shipping, and analytics, which work seamlessly within the platform.

System-Side: RESTful APIs are used to integrate third-party services, facilitating secure and standardized data exchange across modules.

5. Data Storage Location

User-Side: Users’ data is stored within designated regions to comply with local regulations and data sovereignty laws.

System-Side: Customer data storage adheres to geographic and regulatory requirements, ensuring compliance with data sovereignty laws.

---

3.8 Logical Database Requirements

1. Database Type

User-Side: Users’ structured information, like profiles and order details, is stored reliably for consistency across interactions.

System-Side: A relational database (e.g., MySQL) is used for structured data; a NoSQL database (e.g., MongoDB) may store unstructured data, such as logs.

2. Data Requirements

User-Side: Users can access profiles, product details, order histories, and activity logs accurately.

System-Side: Database tables include structured records for user profiles, product details, orders, and transaction logs, organized to support query efficiency.

3. Data Retention

User-Side: Users’ active data remains accessible while their accounts are active, and archived appropriately upon deletion.

System-Side: Customer data retention policies align with account activity and regulatory standards, archiving deleted accounts and maintaining transaction records.

4. Data Formats

User-Side: Users see consistent text, dates, and prices formatted uniformly across the platform.

System-Side: Data is stored in UTF-8 for text, ISO 8601 for dates, and standardized currency formats for prices.

5. Data Integrity

User-Side: Users interact with reliable data relationships (e.g., accurate order and user linkages).

System-Side: The system enforces data integrity via foreign key constraints, ensuring all transactions comply with ACID properties.

---

3.9 Other Requirements

1. Compliance

User-Side: Users’ personal and payment information are protected, meeting GDPR and PCI DSS compliance standards.

System-Side: The system adheres to data privacy and security requirements, ensuring compliance with GDPR and PCI DSS for sensitive data.

2. Supportability

User-Side: Users benefit from a reliable and regularly updated platform that addresses evolving requirements.

System-Side: The codebase is modular and well-documented, designed for easy maintenance and updates.

3. Limitations

User-Side: Users can initially only pay by card, and international shipping may be restricted based on location.

System-Side: The platform currently supports only credit/debit card payments through secure gateways and limits international shipping due to logistical constraints.