Sensitive Data Analysis in a Fictional Organization by Sahil Jain

Identify and Classify Sensitive Data

Part (a) and (b)

Human Resources (HR):

- Personal Identifiable Information (PII): Employee names, addresses, social security numbers, birth dates.
- Payroll Information: Salary, bonuses, tax information.
- Health Information: Medical records or disability status (if any).
- Performance Reviews: Employee evaluations and feedback.
- Employee Benefits: Data related to retirement accounts, insurance, and other benefits.

Finance:

- Financial Reports: Annual reports, balance sheets, profit and loss statements.
- Payroll Information: Employee salaries, bonuses, and tax deductions.
- Banking Information: Company bank accounts, transactions.
- Investment Data: Details about investments and stock holdings.
- Tax Information: Filing records, tax return data.

Research and Development (R&D):

- Intellectual Property (IP): Patents, designs, trade secrets, and proprietary software code.
- Client Project Information: Detailed project requirements and specifications.
- Research Data: Raw data from studies, experiments, or prototypes.
- Business Strategies: Future product development and market strategies.
- Software Architecture: Detailed designs and codebase information.

Customer Support:

- Customer Data: Customer names, contact info, order history.
- Service Requests: Tickets and logs of customer support interactions.
- Feedback Data: Reviews, complaints, or suggestions from customers.
- Transaction History: Details of purchases or subscriptions.
- Account Information: Credentials, account status, billing info.

Sales and Marketing:

- Client Data: Personal contact details, lead information, and customer profiles.
- Sales Data: Revenue, quotas, and sales performance records.

- Marketing Campaign Data: Effectiveness, strategy, and customer response.
- Contracts: Signed agreements with clients and partners.
- Competitive Data: Information on competitors' products or strategies.

Part (c)

Human Resources:
- High: Personal Identifiable Information, Payroll Information.
- Medium: Performance Reviews, Employee Benefits.
- Low: Health Information (only if non-sensitive or generic).

Finance:
- High: Financial Reports, Banking Information, Tax Information.
- Medium: Payroll Information, Investment Data.
- Low: None (since most finance data is high or medium sensitivity).

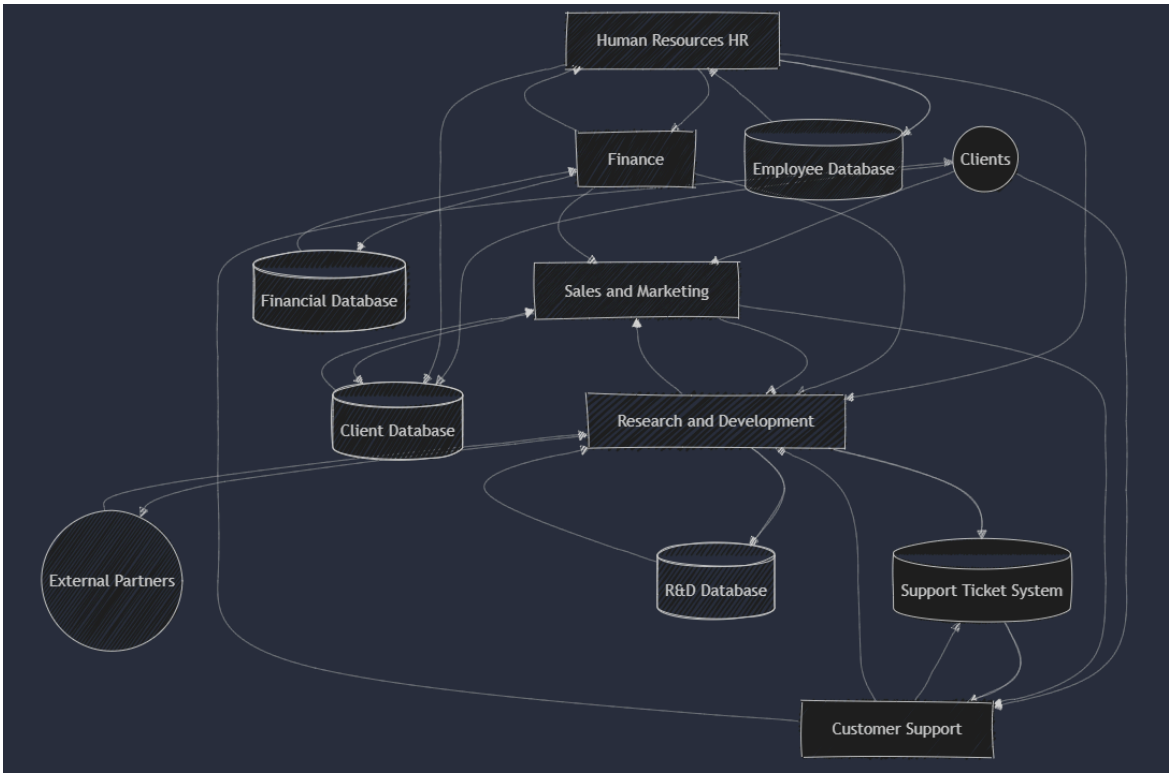
Research and Development:
- High: Intellectual Property, Software Architecture.
- Medium: Client Project Information, Business Strategies.
- Low: Research Data (unless it’s proprietary).

Customer Support:
- High: Customer Data (if it includes sensitive PII or financial info).
- Medium: Service Requests, Feedback Data.
- Low: Transaction History, Account Information (non-sensitive).

Sales and Marketing:
- High: Client Data (especially with financial info), Contracts.
- Medium: Sales Data, Marketing Campaign Data.
- Low: Competitive Data (unless it’s confidential).

Map Data Flows and Risk Points

Part (a)



Part (b)

Risk Point 1: External Partners to R&D Database
Scenario: Sensitive proprietary information, such as software designs and algorithms, is shared with external partners via insecure channels.
Potential Issue: Without proper encryption or secure collaboration tools, this data could be intercepted during transmission or improperly accessed by unauthorized parties.
Risk Point 2: Clients to Sales and Marketing
Scenario: Client data, including personal information or purchase history, flows into the Sales and Marketing department for campaign planning.
Potential Issue: Unrestricted access or inadequate segregation of duties in the department could lead to internal misuse or accidental exposure.
Risk Point 3: Customer Support to Support Ticket System
Scenario: Customer Support collects sensitive client data (e.g., payment information, medical records for healthcare clients) to resolve issues.
Potential Issue: If the Support Ticket System lacks adequate access controls or logging, sensitive data could be mishandled or accessed by unauthorized personnel.

Part (c)

1. External Partners to R&D Database

- **Risk:** Interception of proprietary data.
- **DLP Control:**
    - Implement **end-to-end encryption** for all communications with external partners.
    - Use **secured collaboration tools** (encrypted file-sharing platforms like Box Shield or Microsoft SharePoint with enhanced DLP features).
    - Establish **third-party access agreements** that define data protection expectations and penalties for breaches.

2. Clients to Sales and Marketing

- **Risk:** Misuse of client data.
- **DLP Control:**
    - Enforce **role-based access controls (RBAC)** so that only authorized personnel can view client data.
    - Set up **data masking techniques** for non-essential information.
    - Conduct **regular audits** to ensure compliance with data protection policies and prevent unauthorized access.

3. Customer Support to Support Ticket System

- **Risk:** Improper handling or unauthorized access to sensitive client information.
- **DLP Control:**
    - Implement **logging and monitoring** to track all access and changes made to the Support Ticket System.
    - Configure **automatic data redaction** for highly sensitive fields in tickets.
    - Conduct **ongoing security awareness training** for Customer Support staff to prevent accidental mishandling of sensitive data.