

**School of Computing, Engineering and Physical Sciences**

**MSc Information Technology**

**COMP11113 Information Systems Analysis and Design**

**GROUP COURSEWORK 1 (10% of the marks)**

**Session 2024/2025 Term 1**

**Students**

1. Prajwalaradhya Shivakumaraswamy Kesaramadu (B01759301)
2. Aman Misra (B01746656)
3. Sreeraj Karuvanthodi Ramachandran (B01764963)
4. Muhammed Ali Panthalingal (B01755979)

Lecturer: Raja Ujjan, Ashraf Mahmud

Submission Date: 21-11-2024

**Declaration**

We, the undersigned, do hereby want to state that the work conducted in this project is the outcome of our group efforts and has been accomplished independently. All ideas, data, references, and materials from external sources have been properly cited and acknowledged according to academic standards.

We certify that no member of our group has committed any breach of academic integrity, such as plagiarism, collusion, or contract cheating, in the preparation of this work. Moreover, we declare that this work has not been submitted, in whole or part, for any other course, degree, or qualification at this or any other institution, except where explicitly permitted to do so by the relevant authority.

We understand that any breach of this promise shall be subject to academic penalties and hereby reaffirm our commitment to the policies of this university on academic integrity and honest scholarship.

Table of Contents

[**Table 1** PRIVACY / SECURITY CONCERNS 4](#_Toc182301853)

[**Table 2** ACTIONS TO BE TAKEN BY THE SYSTEM 5](#_Toc182301854)

[References 6](#_Toc182301855)

# **Table 1** PRIVACY / SECURITY CONCERNS

|  |  |
| --- | --- |
| **Privacy/Security Concern** | **Stakeholder(s)** |
| 1. Customer data should be accurate and must not be outdated or inaccurate and not to store longer than required. | Customers,  Store managers |
| 2. We need to make sure that all important business data can be recovered if a disaster occurs. | Store managers  IT Team  Customers |
| 3. Personalized ads, offers, and data tracking can make customers feel like they are being monitored. | Customers |
| 4. Protecting customer contact information is essential for maintaining trust and compliance with data protection regulations. | Customers  Store managers |
| 5. The "chilling effect" occurs when customers modify their behavior because they are aware of digital surveillance, causing disengagement and self-censorship. | Store managers  Store clerk  Customers |
| 6. Accessing data without permission and without a legitimate job-related need. | Store clerk  Customers |
| 7. Securing customer’s financial data. | Store managers  Customers |
| 8. Unauthorized system access can lead to data breaches, which can lead to loss of confidentiality, integrity, and availability of sensitive information. | Store managers  Store clerk  Customers  IT Team |
| 9. Customers should be informed about the intended uses of their data. | Customers  Store managers |
| 10. Unauthorized modification and misusing the data cannot be identified without proper monitoring. | Customers  Store Clerk  IT Team |

# **Table 2** ACTIONS TO BE TAKEN BY THE SYSTEM

|  |  |  |
| --- | --- | --- |
| **Privacy/**  **Security Concerns** | **System Action** | **Is It Illegal/ Unfair?** |
| 1. | Collection of data should be regularly updated, maintained such as phone, email, address etc. Also, not to store it when no longer necessary. | No |
| 2. | Creating backup of all the required data and stored in multiple locations with redundancy is important for ensuring data recovery. | No |
| 3. | Data tracking should occur only when necessary, such as for sending notifications or reminders. This method minimizes unnecessary collection of data improves user privacy. | No |
| 4. | Storing and retrieving contact information only when necessary, such as during customer interactions is crucial for protecting sensitive data. | No |
| 5. | Minimizing unnecessary data collection, increasing transparency about the data processing methods. This approach ensures compliance with data protection rules & regulations. | No |
| 6. | Implementing RBAC (Role-Based-Access-Control) to the system allows more fine-grained access to business data enhancing security and reducing risk of data leak. | No. |
| 7. | Encrypting critical payment information, such as card details and PINs, is vital for data security. Algorithms like AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) provide efficient symmetric encryption. | No |
| 8. | Implementing Multi-Factor Authentication (MFA) for staff members can significantly reduce the risk of data breaches. | No |
| 9. | Organizations should provide transparent privacy policies that clearly outline how customer data is collected, used, processed, and protected. This transparency shows trust and ensures compliance with data protection regulations. | No |
| 10. | Maintaining audit trails and logs provides clear view of who has accessed the data for what purpose. Regularly reviewing logs can help detect unwanted activities. | No |

# References

J. Strycharz and C. M. Segijn, "Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns, and regulatory differences on chilling effects," *Journal of Business Research*, vol. 173, p. 114490, 2024. doi: [10.1016/j.jbusres.2023.114490](https://doi.org/10.1016/j.jbusres.2023.114490).

H. Taherdoost, "Navigating the ethical and privacy concerns of big data and machine learning in decision making," *Intelligent and Converged Networks*, vol. 4, no. 4, pp. 280–295, 2023. doi: [10.23919/ICN.2023.0023](https://doi.org/10.23919/ICN.2023.0023).