**COMP11113 Information Systems Analysis and Design**

University of the West of Scotland, London Campus

Lecturers: Raja Ujjan, Ashraf Mahmud

**COURSEWORK 1**

Students Name:

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

Submission Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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.

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table of Contents

[**Table 1** PRIVACY / SECURITY CONCERNS 4](#_Toc182295666)

[**Table 2** ACTIONS TO BE TAKEN BY THE SYSTEM 5](#_Toc182295667)

[References 6](#_Toc182295668)

# **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 Customer data should be accurate and must not be outdated or inaccurate and not to store longer than required | Customers,  Store managers |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. All critical data related to business should be recoverable if disaster happens | 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’s contact information | Customers  Store managers |
| 5. Change of behaviour of customers when they feel being tracked (Chilling effect) | Store managers  Store clerk  Customers |
| 6. Unauthorised access to data which is not required for their job function | Store clerk  Customers |
| 7. Securing customer’s financial data | Store managers  Customers |
| 8. Unauthorized access to the system lead to data breach or loss. | Store managers  Store clerk  Customers  IT Team |
| 9. Customers should be aware for what purpose data is used for | 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. | No |
| 3. | The data should be tracked only when there is a requirement for ex. Sending notifications/reminders. | No |
| 4. | Storing/Retrieving contact information when there is a need for it. | No |
| 5. | Minimizing unnecessary data collection, increasing transparency about their data processing methods. | No |
| 6. | Implementing RBAC (Role-Based-Access-Control) to the system allows more fine-grained access to business data. | No. |
| 7. | Using Encryption for critical payment information such as card info and pin by using algorithms such AES and RSA. | No |
| 8. | Implementing MFA (Multi-factor authentication) for staff members can significantly reduce the chance of data breach. | No |
| 9. | Organizations should provide clear privacy policies and how data is being used. | 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).