Shivakumaraswamy Kesaramadu - Prajwalaradhya - B01759301.docx

by Prajwalaradhya Shivakumaraswamy Kesaramadu

Submission date: 21-Nov-2024 03:32PM (UTC+0000)

Submission ID: 243343726

File name: Shivakumaraswamy_Kesaramadu_-_Prajwalaradhya_-_B01759301.docx (59.96K)

Word count: 1016

Character count: 6039

UNIVERSITY OF THE WEST *of* SCOTLAND

UWS

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

I have carefully read and fully understand Regulations 3.49–3.55 of Chapter 3 of the Regulatory Framework of the University of the West of Scotland, which outline the rules and policies regarding cheating and plagiarism.

I confirm that this assessment is the collective work of our group, consisting of five members, with each member contributing to the completion of this task. Where applicable, we have clearly referenced and acknowledged the contributions or ideas of others outside our group.

I also affirm that no part of this assessment has been written, in whole or in part, by anyone outside the group, except for explicitly referenced sources.

Furthermore, I confirm that this assessment has not been submitted previously, either partially or fully, for any other module or academic purpose, ensuring it does not fall under self-plagiarism.

This declaration is made with honesty and integrity in adherence to the University's academic standards.

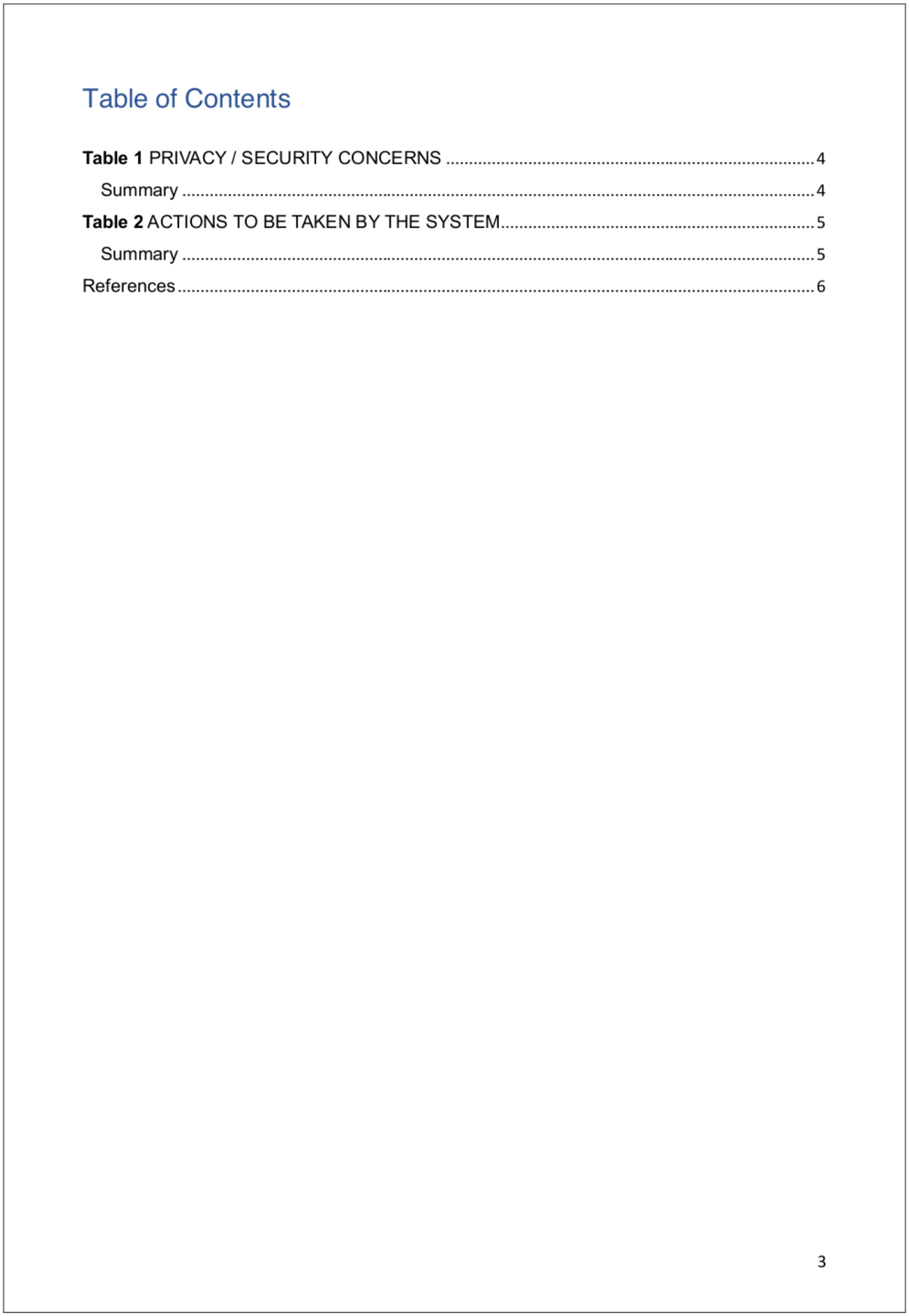

Table of Contents

Table 1 PRIVACY / SECURITY CONCERNS

Privacy/Security Concern	Stakeholder(s)
1. Keep Customer Records Clean and Up-to-Date.	Customers, Store managers
2. Make Sure Business Data is Safe and Recoverable.	Store managers IT Team Customers
3. Don't Make Customers Feel Watched.	Customers
4. Protect Contact Information to Build Trust.	Customers Store managers
5. Avoid Scaring Customers into Changing Their Habits.	Store managers Store clerk Customers
6. Access Only What You Need to Do Your Job.	Store clerk Customers
7. Keep Payment Details Secure.	Store managers Customers
8. Stop Unauthorized Access Before It Causes Damage.	Store managers Store clerk Customers IT Team
9. Be Transparent About How Customer Data is Used.	Customers Store managers
10. Monitor Activity to Prevent Data Misuse	Customers Store Clerk IT Team

Summary

1. Customer records, such as contact information and rental history, should be accurate and must not be outdated or inaccurate and not to store longer than required.
2. We need to make sure that all important business data including rental transactions, supplier information can be recovered if a disaster occurs.
3. Personalized ads, offers, and data tracking such as notification new arrivals, overdue DVDs can make customers feel like they are being monitored (Hamed Taherdoost, 2023).
4. Protecting customer contact information is essential for maintaining trust and compliance with data protection regulations.
5. The "chilling effect" occurs when customers modify their behavior because they are aware of digital surveillance, causing disengagement and self-censorship (Strycharz and Segijn, 2024).
6. Accessing DVD's and customer data without permission and without a legitimate job-related need.
7. Customer payment details like bank cards must be securely stored and protected from unauthorized access.

8. Unauthorized system access can lead to data breaches, which can lead to loss of confidentiality, integrity, and availability of sensitive customer information, DVD rental history, contact details.
9. Customers should be informed about the intended uses of their data where sending overdue notifications, personalized DVD offers.
10. Unauthorized modification and misusing the critical data cannot be identified without proper monitoring.

Table 2 ACTIONS TO BE TAKEN BY THE SYSTEM

Privacy/ Security Concerns	System Action	Is It Illegal/ Unfair?
1.	Regularly Update and Maintain Customer Data.	No
2.	Ensure Backups for Reliable Data Recovery.	No
3.	Limit Data Tracking to What's Essential	No
4.	Securely Store and Access Customer Contact Information.	No
5.	Be Transparent and Avoid Unnecessary Data Collection.	No
6.	Protect Data with Role-Based Access Control (RBAC).	No.
7.	Encrypt Sensitive Payment Information.	No
8.	Use Multi-Factor Authentication for Better Security.	No
9.	Share Transparent Privacy Policies with Customers.	No
10.	Monitor and Review Audit Trails for Security	No

Summary

1. Customer data, including phone numbers, email addresses, and home addresses, should be regularly updated and retained only for the duration required for rentals, notifications, or other necessary purposes.
2. Backing up all essential business data, like rental transactions and supplier details, with redundancy and storing it securely in multiple locations ensures the store can recover quickly and reliably from system failures.
3. Tracking data should only be done when necessary, such as sending overdue DVD reminders or notifying customers about reserved DVDs. This reduces unnecessary data collection and protects privacy.
4. Customer contact details should only be accessed when required for tasks like processing a rental or contacting for overdue DVDs. This helps prevent unauthorized access to sensitive information.
5. Only collect customer data that's absolutely necessary, like what's needed for rentals or notifications. Be open and clear about how this information is used and processed, so customers feel confident their data is handled responsibly. This not only builds trust but also ensures the store follows data protection laws.

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.
7. Encrypting sensitive payment data, such as bank card details, using robust encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) protects against theft or unauthorized access.
8. Implementing Multi-Factor Authentication (MFA) for staff members can significantly reduce the risk of data breaches.
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.
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.

References

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

Hamed Taherdoost (2023). Navigating the Ethical and Privacy Concerns of Big Data and Machine Learning in Decision Making. *Intelligent and converged networks*, 4(4), pp.280–295. doi:https://doi.org/10.23919/icn.2023.0023.

Shivakumaraswamy Kesaramadu - Prajwalaradhya - B01759301.docx

ORIGINALITY REPORT

16%	14%	3%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Goldsmiths' College Student Paper	4%
2	Submitted to University of Northampton Student Paper	3%
3	www.coursehero.com Internet Source	3%
4	Submitted to American Public University System Student Paper	1%
5	waywithwords.net Internet Source	1%
6	whippetnotes.com Internet Source	1%
7	Submitted to The University of the West of Scotland Student Paper	1%
8	www.strongdm.com Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		