AGUMA DESTINY KAMPUMURE

A94163

S21B23/010

1. **Define normalization and how it has been applied in my project**

Normalization is the process of organizing data in a database. This includes creating tables where I was able to create five table and insert data into them, establishing relationships between those tables where some were joining tables hence creating the ability to link several table using foreign keys according to rules designed both to protect the data and to make the database more flexible by eliminating redundancy and inconsistent dependency.

2. **Define the different transaction anomalies giving examples from your project and how they can occur.**

Anomalies are caused when there is too much redundancy in the database's information and the tables that make up the database suffer from poor construction.

There are mainly three types of anomalies in databases namely;

Update anomaly: In my database table we I had two rows for intakes where Ashaba Jasper had been assigned to two intakes which wasn't possible since each on student had to be assigned to one intake strictly. The one under which they were registered in regardless of having been able to attend classes in another. If I want to update the intake of Jasper then we have to update the same in two rows or the data will become inconsistent. If somehow, the correct intake gets updated in one intakes column but not in other then as per the database, Jasper would be having two different intakes, which is not correct and would lead to inconsistent data.

Insert anomaly: New students joined the semester midway in the trinity intake, who are undergoing several classes to catch up then we would not be able to insert the new data into the table if intakes field doesn't allow nulls.

Delete anomaly: Certain students left the department due to one reason or another and were not able to continue with studies so I had to delete their information in all the table.

3. **Suggest ways in which the security of your database is enhanced**.

1. Protect the data itself, not just the perimeter; Concentrating on securing the firewalls technology around the data seems.

2. Pay attention to insider threats; It's easy to visualize threats originating from outside your organization, as these are often represented in news and television as the biggest and most costly ones. However, the reality is that it's your insiders that can potentially hurt you the most because their attacks are much harder to detect and prevent as well.

3. Encrypt all devices; Make sure that all data is stored in an encrypted format and remains encrypted during communications.

4. Testing your security; Installing an antivirus on every computer or device will not protect computer from attacks. Hiring a professional organization to conduct a security audit will always reveal weaknesses you weren't expecting.

5. Delete redundant data; Ensure information disposal mechanisms are in place. It helps prevent stale data from being forgotten about and stolen at a later date.

6. Spending more money and time on Cyber-security; Spend more money and more time on data security as the lack of it continues to be the number one risk.

7. Establish strong passwords; Implementing strong passwords is the first step you can take to strengthen your security in this area. Use reasonably complex passwords and change them at least every 90 days. Don't ever write down your passwords and leave them on your workstation for other people to find.

8. Update your programs regularly; Make sure your computer is properly patched and updated. This is often the best way to ensure its adequately protected. Security applications are only as good as their most recent update.

9. Back-up your data regularly; This should already be a crucial part of any IT security strategy. With secure backups in place, you can survive everything from accidental file deletion to a complete ransomware lockdown. Backup data should be stored in a secure, remote location away from your primary place of business.

10. Create a security mindset; Everyone who has a password and username is responsible for keeping data secure.