**Grandfield College Scenario Module 8 Assignment**

As with any database, data integrity is important to the software database at Grandfield College. If the data are audited, they have to show that they know what software they have, how it is licensed, and on which machines it is installed. Accident and error are the most likely threats to their data integrity, but it is always possible that someone might try to purposely disrupt their data.

1. Create tables of the data access needs of your users.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Administration* |  | |  | | |  | |  | |  | |
| **Table Name** | | **SELECT** | | **INSERT** | | | **UPDATE** | | **DELETE** | | **Constraints** |
| Computers | | X | | | X | | X | | X | |  |
| Computer Users | | X | | | X | | X | | X | | FK Computers\_Key references Computers(Computers\_Key) |
| Faculty / Staff | | X | | | X | | X | | X | |  |
| Departments | | X | | | X | | X | |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *IT Department* |  |  | |  |  |  |
| **Table Name** | **SELECT** | **INSERT** | | **UPDATE** | **DELETE** | **Constraints** |
| Faculty / Staff | X | | X | X |  |  |
| Computers | X | | X | X |  |  |
| Computer Users | X | | X | X | X | FK Computers\_Key references Computers(Computers\_Key) |
| Software | X | | X | X |  |  |
| Software Version | X | | X | X |  | FK Software\_Key references Software(Software\_Key) |
| Software Installation | X | | X | X |  | FK Software\_Version\_Key references Software\_Version(Software\_Version\_Key) |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Faculty / Staff* |  | |  | | |  | |  | |  | |
| **Table Name** | | **SELECT** | | **INSERT** | | | **UPDATE** | | **DELETE** | | **Constraints** |
| Computers | | X | | | X | |  | |  | |  |
| Computer Users | | X | | | X | |  | |  | | FK Computers\_Key references Computers(Computers\_Key) |
| Software | | X | | |  | | X | |  | |  |
| Software Version | | X | | |  | |  | |  | | FK Software\_Key references Software(Software\_Key) |

2. Create a security plan that includes authentication and authorization and general policies and procedures. Consider the use of roles, stored procedures, views, and other tools.

The security plan could vary a great deal here, but a few main points would be:

* Regularly require users to update their password
* Grant specific permissions based on faculty/staff roles to ensure users only access data on their specific computers that they are authorized to.
* Store passwords securely using hashing to ensure the data is secure

3. Documentation: Document and define all the aspects of your plan.

This should consist of a more full explanation of something like the above.

4. Create a preliminary threat analysis.

|  |  |
| --- | --- |
| **Role** | Administration |
| **Threat** | **Description** |
| SELECT | No real threat here |
| INSERT | Insertion errors in Software, Software\_Version\_Number,Software\_Installation |
| UPDATE | Update errors, even catastrophic ones, in Software, Software\_Version, Software\_Version\_Number |
| DELETE | Deletion errors in Software, Software\_Version\_Number |

|  |  |
| --- | --- |
| **Role** | IT Department |
| **Threat** | **Description** |
| SELECT | No real threat here |
| INSERT | Insertion errors in Software, Software\_Version\_Number,Computer\_Users |
| UPDATE | Update errors, even catastrophic ones, in Software , Computer\_Users |
| DELETE | Deletion errors in Software , Computer\_Users |

5. Make a preliminary disaster management plan.

The response should use the threat tables and contain some discussion. The most dangerous user is certainly the IT department because they do most of the data entry and data maintenance. There should be no public access at all. Any public access would be through malicious attack.

Internal Threats:

* Accidental data deletion/updates or modification by IT department
* Unauthorized data access by faculty/staff or administration

External Threats:

* Cyber-attacks from faculty/staff computer usage (ex. email phishing/virus)
* Data breaches and unauthorized access to faculty/staff computers.

In order to have a safe and secure database the college should focus on maintaining a strong authentication and authorization system and regularly update software to lessen the likelihood of vulnerabilities/database failure.

6. Create a view of the data that is tailored to the needs of one of your uses.

*-- Create a view for IT Department data authorization based on their access*

CREATE VIEW IT\_Department\_Authorization AS

SELECT

Computer\_Users.User\_Information AS 'User Contact Information',

Software.Software\_Type AS 'Software Type',

Software\_Installations.Software\_Installation\_Number AS 'Software Installation Number',

Software\_Version.Version\_Number\_ID AS 'Version Number',

Computers.Computers\_ID AS 'Computer ID'

FROM

Software\_Installations

JOIN

Computers ON Software\_Installations.Computers\_Key = Computers.Computers\_Key

JOIN

Computer\_Users ON Computers.Computers\_Key = Computer\_Users.Computers\_Key

JOIN

Software\_Version ON Software\_Installations.Software\_Version\_Key = Software\_Version.Software\_Version\_Key

JOIN

Software ON Software\_Version.Software\_Key = Software.Software\_Key;

*-- Display the specified data from the IT\_Department\_Authorization view*

SELECT \* FROM IT\_Department\_Authorization;