CSC 544/744: Database Administration & Security
Homework Assignment 7 (Term Project)
(25 points)
Today's Date: Tuesday, November 14

Consider a simplified database application for a college:

1. The database should provide access to the following groups of accounts:

User Account	Related Information	Password
App_Admin	Application administrator	AA1234
App_Schema	Application schema	AS1234
LayJ …	Staff in Registrar's Office	L1234
DavisC …	Student	D1234
YangM …	Instructor	Y1234

   - App_Schema is the account that owns the tables for this database application.
   - App_Admin manages user accounts, privileges, roles, and implement security policies for this database.

2. The database contains the following tables:

STUDENTS

Column Name	Data Type and Constraint
ID	NUMBER(9, 0) PRIMARY KEY
LAST_NAME	VARCHAR2(30)
FIRST_NAME	VARCHAR2(30)
ENAME	VARCHAR2(31) UNIQUE
MAJOR	VARCHAR(25)

INSTRUCTORS

Column Name	Data Type and Constraint
ID	NUMBER(9,0) PRIMARY KEY
LAST_NAME	VARCHAR2(30)
FIRST_NAME	VARCHAR2(30)
ENAME	VARCHAR2(31) UNIQUE
DEPT	VARCHAR(3)

COURSES

Column Name	Data Type and Constraint
CRN	NUMBER(5, 0) PRIMARY KEY
INSTRUCTOR_ID	NUMBER(9, 0)

ENROLLMENT

Column Name	Data Type and Constraint
STUDENT_ID	NUMBER(9, 0)
CRN	NUMBER(5, 0)
GRADE	NUMBER(4)

- ENAME is a virtual column. Its value derives from LAST_NAME and FIRST_NAME, by including the last name followed by the first letter of the first name. Assume all people using this database application have different ENAME values.

3. The database should enforce the following security policies that specify who are allowed to do what on the database objects:

Policy No.	Who	What
1	Staff member in the Registrar's Office	Insert records into any of the above tables
2	Staff member in the Registrar's Office	Delete records from any of the above tables
3	Staff member in the Registrar's Office	View any record in any of the above tables
4	Staff member in the Registrar's Office	Update any record in any of the above tables
5	Student	View his/her own record in STUDENTS table
6	Student	View all information in INSTRUCTORS table except for IDs
7	Student	View all information in COURSES table
8	Student	View his/her own records in ENROLLMENT table
9	Instructor	View all records in STUDENTS table
10	Instructor	View rows for other people in INSTRUCTORS table except for IDs
11	Instructor	View his/her row in INSTRUCTORS table including ID
12	Instructor	View all information in COURSES table
13	Instructor	View all records in ENROLLMENT table
14	Instructor	Update his/her own record in INSTRUCTORS table except for the ID and ENAME
15	Instructor	Update the grades of students in the courses that he/she teaches

Part I (10 points): Analysis (Due: *Tuesday, November 26*)

1. Outline the approach you are planning to use in order to enforce each of the above required security policies by filling in the table below, and describe the auxiliary approaches if any.

	Approach
Policy 1	
Policy 2	
Policy 3	
Policy 4	
Policy 5	
Policy 6	
Policy 7	
Policy 8	
Policy 9	
Policy 10	
Policy 11	

Policy 12	
Policy 13	
Policy 14	
Policy 15	

2. Document the privileges/roles that each role/user should be granted by filling in the table below.

Grantee	Type	Privilege/Role	Object Shema	Object Name	Column Name	Grantable	Grantor
.....							

- Type: indicates the grantee is a database user account or a role
- If the granted privilege is an object privilege, you need to document the privilege applies to which columns of which objects in which schema
- Grantable: indicates whether the grantee of the privilege can pass on the privilege to other roles/users

What to submit

Word or PDF file.

Part II (3+2+10 points): Implementation (Due: *Friday, December 6*)

1. Create user accounts
2. Create necessary database objects (tables, views, ….)
3. Implement the required security policies
   - CSC 545: Need to implement 10 of the security policies correctly in order to get full credits. One and half extra credit will be awarded for each additional security policy implemented.
   - CSC 745: Need to implement 10 of the security policies correctly, in order to get full credits. One of those 10 you choose to implement must include policy 15. One and half extra credit will be awarded for each additional security policy implemented.

What to submit

- SQL Script file(s) to create user accounts, database objects, and implement security policies.
- README file to briefly explain how to use the script files to set everything up.