



Strathmore
UNIVERSITY

**SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
MASTER OF SCIENCE IN INFORMATION SYSTEM SECURITY
END OF SEMESTER EXAMINATION
MST8302 – ENTERPRISE SECURITY**

DATE: 12th October 2022

Time: 2 Hours

Instructions

1. This examination consists of **SEVEN** questions. You can get up to **40 points**.
2. Answer **all** the questions.
3. For each question, provide the answers according to the **instructions in brackets** (the instructions describe a style of the answers and how long each should be).

Questions

1. Describe IT security concepts of Authorization, Accounting, and Authentication. In which order these concepts have to be implemented and why? Provide an example. **(6 points)**
2. Briefly describe the four basic access control models: Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), and Rule Based Access Control (RBAC or RB-RBAC). **(8 points)**
3. Describe three different strategies on where Authentication and Authorization (AA) of a user should be performed (i.e., AA at application/database levels; both AA at one of these levels, as well as each of AA at different levels). What are advantages and disadvantages of these strategies? Also describe the concept of a "proxy user" in the case of Authentication at the application level and Authorization at the database level strategy. **(8 points)**
4. Why do we need Fine-grained Access Control in database security (why SQL Data Control Language statements are not good enough) and how it can be implemented in Virtual Private Databases (two approaches)? **(5 points)**
5. What is the purpose of Data Masking and Data Redaction and how they affect query results? Are there any differences between these two? Provide examples. **(4 points)**
6. What is Polyinstantiation and Cover Stories? Why and how the polyinstantiation can be used to secure private information? **(5 points)**
7. What are Control Columns in relational database tables? Provide at least three examples of different control columns and explain how they can be utilized in database audit. **(4 points)**