NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS (INFORMATION SECURITY)	
QUALIFICATION CODE: 08BHIS	**LEVEL:** 8
COURSE: Database Security and Data Protection	**COURSE CODE:** DSD821S
DATE: JANUARY 2020	**SESSION:** 2
DURATION: 3 hours	**MARKS:** 100

SUPPLEMENTARY/SECOND OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**MR. ISAAC NHAMU**
MODERATOR:	**DR. AMELIA PHILLIPS**

THIS QUESTION PAPER CONSISTS OF 5 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions you should be guided by the allocation of marks in [ ]. Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. Non programmable Scientific Calculator.

SECTION A (Multiple Choice questions – 10 marks)

1. A single-user database system automatically ensures ____ of the database, because only one transaction is executed at a time.

   A. serializability and durability
   B. atomicity and isolation
   C. serializability and isolation
   D. atomicity and serializability

2. What is a rule that applies to the two-phase locking protocol?

   A. Two transactions cannot have conflicting locks.
   B. No unlock operation can precede a lock operation in a different transaction.
   C. No data is affected until all locks are released.
   D. No data is affected until the transaction is in its locked position.

3. All transactions must display ____.

   A. atomicity, consistency, and durability
   B. durability and isolation
   C. consistency, durability, and isolation
   D. atomicity, durability, consistency, and isolation

4. The information stored in the ____ is used by the DBMS for a recovery requirement triggered by a ROLLBACK statement, a program's abnormal termination, or a system failure such as a network discrepancy or a disk crash.

   A. data dictionary
   B. metadata
   C. rollback manager
   D. transaction log

5. A ____ is a named collection of database access privileges that authorize a user to connect to the database and use the database system resources.

   A. user
   B. role
   C. profile
   D. manager

6. A ____ is a named collection of settings that control how much of the database resource a given user can use.
   A. Role
   B. Profile
   C. Schema
   D. Manager

7. SQL injection is an attack in which _____ code is inserted into strings that are later passed to an instance of SQL Server.
   A. malicious
   B. redundant
   C. clean
   D. non malicious

8. Which statement is not true?

   A. SQL injection vulnerabilities occur whenever input is used in the construction of an
   B. SQL query without being adequately constrained or sanitized SQL injection allows an attacker to access the SQL servers and execute SQL code under the privileges of the user used to connect to the database
   C. The use of PL-SQL opens the door to these vulnerabilities
   D. None of the mentioned

9. Purpose of DDL Trigger is to:

   A. Perform administrative tasks
   B. Create tables
   C. Regulating database operations.
   D. A and C

10. Which of the following statement is true?

   A. Views could be looked as an additional layer on the table which enables us to protect intricate or sensitive data based upon our needs
   B. Views are virtual tables that are compiled at run time
   C. Creating views can improve query response time
   D. All of the Mentioned

SECTION B

Question 1

a. Give one technique for validation and one for verification. [2]

b. Giving examples describe the following verification, validation and testing techniques: [8]

i. Informal
ii. Formal
iii. Static
iv. Dynamic

Question 2

a. Besides Query Restrictions and Swapping, how can inference be controlled. Outline two methods. [4]

b. Consider the statistical database in Table 2.1. Given that a normal user may not query the database on the field "Name" and may only use formulas such as: `count(C)`, `sum(C,Aj)`, `median(C,Aj)`, `max(C,Aj)`, `min(C,Aj)`, `etc.` `C` is the characteristic formula, such as *(Sex=Male) AND (Department=Math)*. The query set, `X(C)`, is the set of records matching the characteristic formula. $|X(C)|$ is the number of records in this matching set. N is the size of the database (number of rows or records). `Aj` is a specific attribute, such as *Salary*. According to table 2.1, these values then give: `max(C,Aj) = 72.`

Table 2.1

Name	*Sex*	*Department*	*Position*	*Salary (N$1000)*
Barry	Male	CS	Lecturer	80
Abraham	Male	Math	Lecturer	60
Lidia	Female	Math	Lecturer	100
Carmia	Female	CS	Lecturer	60
Hausiku	Male	Stat	Lecturer	72
Johannes	Female	Stat	Lecturer	88
Jekonia	Male	CS	Admin	40
Germanus	Male	Math	Lecturer	72
Emelia	Female	CS	Intern	12
Immanuel	Male	Stat	Secretary	80
Ruth Helao	Female	Math	Lecturer	100
Zacharias	Male	CS	Intern	12
Josephina	Female	CS	Secretary	80

i. Given that C is the formula *(Sex=Female) OR (Position=Lecturer)* and Aj is *Salary* find the values for sum(C,Aj), median(C,Aj), and max(C,Aj). [4]

ii. Explain how the *query size restriction technique* can be used to protect the statistical database from an inference attack. Describe it formally using N and $|X(C)|$ as defined above, and the constant k. [4]

iii. Demonstrate how the *direct attack* could be used to find the exact salary of Secretary Immanuel. [3]

iv. Give an example of how you would implement swapping on the data in table 2.1. [2]

v. What information available to the statistical database user could be distorted by your method in iv? [3]

Question 3

Define at least 10 sets of standards and policies for adding, modifying and removing users from a database. [10]

Question 4

a. An individual may prefer to deal anonymously or pseudonymously with an organisation for various reasons, give at least 4 reasons why this can occur. [4]

b. With regards to personal information what do the following mean:
   i. Implied consent
   ii. Express consent
   iii. Bundled consent [6]

Question 5

a. Discuss, with examples, three types of problems that can occur in a multiuser environment when concurrent access to the database is allowed. [12]

b. The following table shows a schedule of three parallel transactions T_1, T_2 and T_3.

Time	T_1	T_2	T_3
1	read(X)	read(X)	read(Y)
2	X := X- 3		Y := Y + 1
3		read(Y)	
4		X := X + 2	write(Y)
5	read(Z)	write(X)	read(Z)
6	Z:= Z + 1		
7	write(Z)		

i. Using diagram or otherwise, determine whether the schedule above is serializable or not. [8]

Question 6

a. Describe seven ways of restricting network access in an Oracle database. [14]

b. Write a script to create a profile to be assigned to the user **Ruva** called **SuppExam** that has the following restrictions: [6]

a. Users are logged out after 15minutes of being idle.
b. A user who logs in 4 times with the wrong password is locked out.
c. A password can only be used for 90 days.
d. A password can only be reused 5 times.
e. A user is allowed 7 days to change the password after it has expired.

<<<<<<<<<<< END OF PAPER >>>>>>>>>>