CSEC 5304, **Database Security**
CSEC 3366, **Database Security**

Department of Computing and Cyber Security, College of Business
Course Syllabus
Class Meeting Time and Place: R 5:30 pm - 08:15 PM, Online
Class Duration: 01/21 to 05/13/2025
Instructor: Dr. Izzat Alsmadi, Tel: 210-784-2313 E-Mail: ialsmadi@tamusa.edu
Office Hours:
Tuesday….02:00 pm -0400 pm Online
Thursday…..200 pm – 5:30pm Online

Catalog Course Description:

CSEC 5304: This course focuses on the protection of data at rest. The course covers subjects in databases and DBMS related to security. Examples of subjects include: DB access control and identity management, DB architecture, password policies, DB auditing, privileges, and roles administration.

Prerequisite: CCS Department Approval.

Course Objectives: The objective of the course is:

- Demonstrate understanding of current database technology and typical database products.
- Demonstrate understanding of security architecture in modern computer systems in a typical enterprise.
- Formulate a working definition of database security and administration.
- Identify contemporary practices of operating system security.
- Cover in details the various state-of-art database security methods and techniques.
- Cover in details the security features in databases
- Demonstrate the knowledge and skills for administration of user, profiles, password policies, privileges and roles.
- Manage database security on application level.
- Conduct database auditing for security and reliability.
- Implement typical security projects on enterprise systems.

Learning Outcomes

After completion of the course students are expected to be able to:

- Understand and characterize modern techniques of database information security threats and techniques for database security assessment.
- Analyze information in a database to identify information security incidents
- Understand and use the main tools for database management systems monitoring.
- Use build-in database functions to enable database integrity support.
- Understand and identify database information security threats, critically evaluate and apply the potential countermeasures.
- Create a plan for vulnerabilities detection and identification in databases.
- Reasonably use and analyze the results obtained by the database vulnerability scanners.
- Apply new methods of a database protection and use tools for database security assessment