

## Course Syllabus Part I

### CYBR 410 Data/Database Security

3 Credit Hours

---

#### Course Description

This course focuses on the protection of data at rest. Coverage includes the identification, ownership, and protection of data – whether residing in files, folders, or databases. This course also introduces the concept of database security to include: Architecture, Password Policies, Auditing, Privileges, and Roles Administration. Emphasis is placed on areas unique to data and database security.

#### Course Prerequisites

None

---

#### Course Objectives

Students who successfully complete this course should be able to:

1. Identify the fundamental structures of secure database systems.
2. Discuss the key components of deploying a secure database.
3. Identify how to control data securely and guard against database threats.
4. Assess how modern business structures integrate secure databases.
5. Discuss current tools and methodologies for database assessments.
6. Discuss techniques used by hackers to exploit database flaws and vulnerabilities.
7. Configure database security auditing and testing, covering vendor-specific processes.

---

#### Grading Scale

93 – 100% = A	87 – 89% = B+	77 – 79% = C+	67 – 69% = D+
90 – 92% = A-	83 – 86% = B	73 – 76% = C	63 – 66% = D
	80 – 82% = B-	70 – 72% = C-	60 – 62% = D-
			0 – 59% = F

---

#### Topic Outline

- I. Security and Information Technology
  - a. Database security
  - b. Hackers
  - c. Malware
  - d. Security architecture
  - e. Global policies
  - f. Data identification and classification
- II. Database Review
  - a. Definition

- b. Database structure components
- c. Database models
  - i. Flat
  - ii. Hierarchical
  - iii. Network
  - iv. Relational
  - v. Object-oriented
  - vi. Object-relational
- d. Database types
- e. Database Management Systems (DBMS)
- f. Oracle
- g. MySQL
- h. Microsoft SQL Server
- III. Database Installation – MySQL
  - a. Preinstallation
  - b. Downloading MySQL
  - c. Configuration
  - d. Security suggestions
- IV. Database Installation – Microsoft SQL Server
  - a. Requirements
  - b. Supported platforms
  - c. Software prerequisites
  - d. Installation
  - e. Security considerations
- V. Database Installation – Oracle
  - a. Requirements
  - b. Preinstallation
  - c. Configuration
  - d. Security suggestions
- VI. Password, Profiles, Privileges, and Roles
  - a. Authentication
  - b. Authorization
  - c. Inference
- VII. SQL Injection Identification
  - a. SQL Injections
  - b. Identifying vulnerabilities
- VIII. SQL Injection Exploitation and Defense
  - a. Exploitations and information gathering
  - b. Extracting read data
  - c. Exploiting privileges and passwords
  - d. Defense
- IX. Auditing
  - a. Security auditing
  - b. Database auditing
- X. Security Testing
  - a. Testing
  - b. Methodologies
  - c. Reporting