

**Common Course Outline**  
**DCOM 258**  
**Introduction to Information Security**  
**3 Semester Hours**

**The Community College of Baltimore County**

**Description**

**DCOM 258 – 3 Credits – Introduction to Information Security** explores the field of Information Security and how it relates to other areas of Information Technology (IT). The material covered in this class provides the broad-based knowledge and skills necessary to prepare students for further study in specialized security fields, or may be used by those interested in a general introduction to the field. This course is also intended to serve the needs of those seeking to pass the Computing Technology Industry Association's (CompTIA) Security+ certification.

**3 credits; 3 lecture hours per week**

**Prerequisite: DCOM 101 or consent of the program coordinator**

**Overall Course Objectives**

Upon completion of this course the student will be able to:

1. describe why information security is essential in today's IT environment;
2. identify the goals of information security;
3. describe common security threats and their ramifications;
4. determine the factors involved in developing a secure information security strategy;
5. identify common attacks and describe how to safeguard against them;
6. describe communications, E-mail, Web, remote access, and wireless security issues;
7. evaluate various network devices and media and how best to secure them;
8. describe the basics of cryptography;
9. differentiate between physical security, disaster recovery, and business continuity;
10. describe computer forensics and its role in information security;
11. utilize network diagrams; and
12. demonstrate appropriate and ethical behavior and good work habits.

## **Major Topics**

- I. Information Security Fundamentals
  - a. Identify the challenges for information security
  - b. Define information security
  - c. Describe the importance of information security
  - d. Describe the CompTIA Security+ certification exam and objectives
  - e. Discuss types of information security careers
- II. Attackers and Their Attacks
  - a. Develop attacker profiles
  - b. Describe basic attacks
  - c. Describe identity attacks
  - d. Describe denial of service attacks
  - e. Discuss types of malicious software
- III. Security Basics
  - a. Identify who is responsible for information security
  - b. Describe security principles
  - c. Evaluate effective authentication methods
  - d. Control access to computer systems
  - e. Audit information security schemes
- IV. Security Baselines
  - a. Evaluate nonessential systems
  - b. Harden operating systems, applications, and networks
- V. Securing the Network Infrastructure
  - a. Work with network cable plant
  - b. Secure removable media
  - c. Harden network devices
  - d. Design network topologies
- VI. Web Security
  - a. Protect E-mail systems
  - b. Describe World Wide Web vulnerabilities
  - c. Secure Web communications
  - d. Secure instant messaging
- VII. Protecting Advanced Communications
  - a. Harden File Transfer Protocol
  - b. Secure remote access
  - c. Protect directory services
  - d. Secure digital cellular telephony
  - e. Harden wireless local area networks
- VIII. Scrambling Through Cryptography
  - a. Define cryptography
  - b. Describe various uses of cryptography
  - c. Secure with cryptographic hashing algorithms
  - d. Protect with symmetric encryption algorithms
  - e. Harden with asymmetric encryption algorithms

## **Major Topics (continued)**

- IX. Using and Managing Keys
  - a. Discuss cryptography strengths and vulnerabilities
  - b. Define public key infrastructure
  - c. Manage digital certificates
  - d. Explore key management
- X. Operational Security
  - a. Harden physical security with access control
  - b. Minimize social engineering
  - c. Secure the physical environment
  - d. Discuss business continuity and disaster recovery
- XI. Policies and Procedures
  - a. Discuss the security policy cycle
  - b. Describe risk identification
  - c. Discuss types of security policies
  - d. Design a security policy
  - e. Discuss compliance monitoring and evaluation
- XII. Security Management
  - a. Define and discuss identity management
  - b. Harden systems through privilege management
  - c. Plan for change management
  - d. Define and discuss digital rights management
- XIII. Advanced Security and Beyond
  - a. Define and discuss computer forensics
  - b. Describe responding to a computer forensics incident

## **Course Requirements**

**Grading/exams:** Grading procedures will be determined by the individual faculty member but will include the following:

Minimum of five case projects

Minimum of three exams

**Writing:** The individual faculty member will determine specific writing assignments, such as writing an Acceptable Usage Policy.

## **Other Course Information**

This course is a required course in the revised Web Technology degree program and an elective in the Data Communications (DCOM) and Computer Information System (CINS) degree programs.

Individual faculty members may include additional course objectives, major topics, and other course requirements to the minimum expectations stated in the Common Course Outline.