DCOM 258
Introduction to Information Security

3 Credits

Community College of Baltimore County
Common Course Outline

Description

DCOM 258 – Introduction to Information Security: provides the knowledge and skills required to assess the overall state of the security of an enterprise environment and recommend and implement appropriate security solutions. Students learn to monitor and secure physical and virtual environments and respond to security incidents while operating with an awareness of applicable security-based laws and policies. This course prepares students for the Computing Technology Industry Association's (Comp TIA) Security+ certification.

Pre-requisites: DCOM 101 or consent of the Program Coordinator

Overall Course Objectives

Upon completion of this course, students will be able to:

1. compare security roles and security controls;
2. identify information security competencies;
3. assess the cybersecurity posture of an enterprise environment;
4. discuss cybersecurity framework (CSF) such as the National Institute of Standards and Technology (NIST);
5. perform organizational security assessments using various tools;
6. implement appropriate cybersecurity solutions such as secure network designs, management policies, and personnel training;
7. identify data privacy and protection concepts;
8. execute incident response;
9. perform risk management;
10. implement cryptographic elements and infrastructures;
11. explain key aspects of Digital Forensics needed to create appropriate documentation;
12. monitor and secure physical and virtual environments;
13. identify types of attacks such as ransomware, social engineering, malware, and denial of service;
14. discuss authorization, authentication, and identity controls;
15. operate with an awareness of applicable security laws and policies; and
16. determine an appropriate response to cybersecurity events and incidents.

Major Topics

I. Security Roles and Security Controls
II. Threat Actors and Threat Intelligence
III. Security Assessments and Solutions

IV. Social Engineering and Malware

V. Basic Cryptographic Concepts

VI. Authentication Controls

VII. Identity and Account Management Controls

VIII. Secure Network Designs and Protocols

IX. Network Security Appliances

X. Secure Physical and Virtual Environments

XI. Data Privacy and Protection Concepts

XII. Incident Response

XIII. Digital Forensics

XIV. Risk Management Concepts

XV. Physical Security

<u>Course Requirements</u>

Grading will be determined by the individual faculty member, but shall include the following, at minimum:

- Two exams
- 20 quizzes
- 15 hands on lab projects

Date Revised: 11/16/2021