ATLANTIC CAPE COMMUNITY COLLEGE

ISAS DEPARTMENT

COURSE SYLLABUS

COURSE TITLE: CISM176 - Systems Security Methods

REQUIRED TEXTBOOK AND MATERIALS: Required: TestOut. LabSim for Security Pro (SY0-401/SSCP) online simulation courseware Optional: Ciampa, Security+ Guide to Network Security Fundamentals, 5th Edition, Cengage Learning

COURSE DESCRIPTION:
A study of the fundamental techniques for computer security and its implementation. Students will learn to assess and mitigate risk, evaluate and select appropriate technologies, and apply proper security safeguards. (The course is designed to prepare students for the CompTIA Security+ industry certification exam.)

PRE-REQUISITE:
Introduction to Computers - CISM125

ADA STATEMENT:
As per the Americans with Disabilities Act (ADA), reasonable accommodations can be provided to students who present current documentation (within five years) of a disability to Atlantic Cape Community College's Center for Accessibility, located on the first floor of "J" Building in the Counseling and Support Services department (Mays Landing campus). Reasonable accommodations cannot be provided for a course until the student registers with the Center for Accessibility. For more information, please contact the Center for Accessibility via email at cfa@atlantic.eduor call 609-343-5680.

LEARNING GOALS:

The student will
explore network security
investigate compliance and operational security
assess threats and vulnerabilities
study application, data and host security
examine access control and identity management
understand cryptography

LEARNING OUTCOMES:

Develop and manage a secure network.
Explain risk related concepts concerning compliance and operations.
Analyze and describe assessment tools and techniques to discover security threats and vulnerabilities.
Explain the importance of application, data and host security.
Describe and assess the function and purpose of authentication services.
Summarize general cryptography concepts.

LEARNING OBJECTIVES:

Students will be able to:
Explain the security function and purpose of network devices and technologies
Apply and implement secure network administration principles
Distinguish and differentiate network design elements and components
Implement and use common protocols
Identify commonly used default network ports
Implement wireless network in a secure manner
Explain risk related concepts
Carry out appropriate risk mitigation strategies
Execute appropriate incident response procedures
Explain the importance of security related awareness and training
Compare and contrast aspects of business continuity
Explain the impact and proper use of environmental controls
Execute disaster recovery plans and procedures
Discuss the concepts of confidentiality, integrity and availability (CIA)
Analyze and differentiate among types of malware
Analyze and differentiate among types of attacks
Analyze and differentiate among types of social engineering attacks
Analyze and differentiate among types of wireless attacks
Analyze and differentiate among types of application attacks
Analyze and differentiate among types of mitigation and deterrent techniques
Implement assessment tools and techniques to discover security threats and vulnerabilities
Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning
Explain the importance of application security
Apply out appropriate procedures to establish host security
Explain the importance of data security
Explain the function and purpose of authentication services
Explain the fundamental concepts and best practices related to authentication, authorization and access control
Implement appropriate security controls when performing account management
Summarize general cryptography concepts
Use and apply appropriate cryptographic tools and products
Explain the core concepts of public key infrastructure
Implement PKI, certificate management and associated components

ASSESSMENT STRATEGIES:

Student Learning Outcome	Assessment Strategy
Develop and manage a secure network	Lab
Explain risk related concepts concerning compliance and operations	Lab Exam
Analyze and compare assessment tools and techniques to discover security threats and vulnerabilities	Lab Exam
Explain the importance of application, data and host security	Exam
Describe and assess the function and purpose of authentication services	Exam
Summarize general cryptography concepts	Exam

COLLEGE GRADING SCALE (EXCEPT FOR PARALEGAL, NURSING, AND CULINARY PROGRAMS)

Grade	**Percentage Range**	**Grade Point Value**
A	93-100%	4.0
A-	90-92%	3.7
B+	87-89%	3.3
B	83-86%	3.0
B-	80-82%	2.7
C+	77-79%	2.3
C	70-76%	2.0
D	60-69%	1.0
F	0-59%	0.0