September 2019
(New)

EDINBORO UNIVERSITY OF PENNSYLVANIA
Department of Mathematics and Computer Science

Introduction to Cybersecurity

CSCI 277 3 Credit Hours

Catalog Description:
The course is designed to provide a broad overview of the field of cybersecurity. Through labs and lectures students will be exposed to a variety of security concepts as well as several security vulnerabilities. Prerequisites: enrollment in or completion of CSCI 230, C- or better in CSCI 130 and CSCI 125.

Course Outline:

I. Crosscutting Concepts in Cybersecurity
   A. Confidentiality, integrity, availability
   B. Risk
   C. Adversarial thinking
   D. Systems thinking

II. Software Security
   A. Fundamental design principles for secure software
   B. Security requirements and their role in system design
   C. Implementation issues
   D. Software Testing
   E. Ethics related to development, testing and vulnerability disclosure

III. Component Security
   A. Vulnerabilities of system components
   B. Component life cycle

IV. Connection Security
   A. Introduction to data communications
   B. Network architectures and models
   C. Connection and transmission attacks

V. System access and authentication
   A. Basic Cryptographic Concepts
   B. Authentication Methods
   C. Identity
   D. Attacks and mitigation measures

VI. Human Security
   A. Social engineering
      1. Psychology of Social Engineering Attacks
   B. Awareness and understanding of security issues
      1. System misuse and user misbehavior
      2. Proper behavior under uncertainty
      3. Enforcement and rules of behavior
   C. Privacy
      1. Social and Behavioral Privacy

2. Social Media Privacy and Security

VII. Organizational Security
   A. Risk and risk management
   B. Secure governance and policy
   C. Systems administration

VIII. Societal Security
   A. Cybercrime
   B. Cyber ethics
   C. The role of policy

Course Objectives and Assessments:

Objective	**Assessment (two)**	**Assessment Methods**
1. Describe basic concepts involved with cybersecurity	A. Students will provide standard definitions for terms and concepts related to cybersecurity.	Any of the following assessment methods will be employed: • Homework • Lab work • Group work • Presentations • Reports • Projects • Tests
2. Describe the steps required to produce secure software.	A. Students will name and describe the tasks involved in producing secure software.	
3. Explain how components impact the overall security of a system.	A. Given a standard model of a system, students will identify components and explain how these components impact the security of the system.	
4. Describe basic security issues involved in data communications.	A. Given a standard model of a system involving data communications, students will identify and describe potential vulnerabilities in the system.	
5. Describe methods for accessing a system and their impact on system security.	A. Given a model of an authentication system, students will list potential vulnerabilities in the system.	
6. Discuss issues involved in human security.	A. Given a model of a system and a description of the methods used for human interaction, students will list and describe potential vulnerabilities related to human interaction.	
7. Identify major tools available to organizations to manage cybersecurity.	A. Students will describe various tools organizations can employ to enhance cybersecurity.	
8. Identify and describe major impacts of cybersecurity on society.	A. Students will list and describe several areas in which cybersecurity has an impact on society.	