



Course Syllabus Cover Page — Fall 2025

Course Number: CYS 1100

Course Title: Introduction to Cybersecurity

Credit(s): 3

Prerequisite(s): None.

Course Description:

The students will explore the field of Cybersecurity focusing on the technical and managerial aspects of the discipline. Students will be introduced to the basic terminology, concepts, and best practices of computer/network security and the roles and responsibilities of management/security personnel. The students will learn the technologies used and techniques involved in creating a secure computer networking environment including authentication and the types of attacks against an organization.

Learning Outcomes:

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

1. Define/describe the principles of cybersecurity and the fundamental concepts of the cyber security discipline used to provide system security. (CSF, CSP)
2. Describe potential system attacks and the actors that might perform them. Examine how the internet is used for cybercrime, cyber-stalking, and other abusive behavior. (CSF, CCR)
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks. (CSF, CSP, NSA)
4. Understand the Federal, State and Local Cyber Defense partners/structures. Properly use the Vocabulary associated with cyber security. (CSF, ISC)
5. Examine diverse ethical dilemmas, the role of cybersecurity in supporting and encouraging ethics, and cybersecurity practices that can cause ethical conflicts with the interconnected world. (CSE)
6. Evaluate the effectiveness of applications of cybersecurity in preventing crime and abuse including recommended best security practices on risk assumptions. (NSA)
7. Students will be able to identify the elements of a cryptographic system and describe the differences between symmetric and asymmetric algorithms. (BCY)