Course number and name: **CS 03500: Foundations of Cybersecurity**
Credits and contact hours: 3 credits / 3 contact hours
Course Coordinator: Fred Stinchcombe
Instructional Materials: Principles of Computer Security: CompTIA Security+ and Beyond, Sixth Edition, 2021, Conklin

Specific course information

Catalog description: This course exposes students to the principles of cybersecurity and will introduce a wide range of security activities, methodologies, and procedures. The topics covered in the course include fundamental concepts of computer security, principles of cryptography, software security and trusted systems, network security as well as other topics.

Prerequisites: None

Type of Course: ☒ Required ☐ Elective ☐ Selected Elective

Educational objectives for the course:

- Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
- Describe potential system attacks and the actors that might perform them
- Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
- Describe appropriate measures to be taken should a system compromise occur.
- Properly use the Vocabulary associated with cybersecurity.
- Define the principles of cybersecurity.
- Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
- Analyze common security failures and identify specific design principles that have been violated.
- Given a specific scenario, identify the design principles involved or needed.
- Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.
- Describe the hardware components of modern computing environments and their individual functions.
- Describe the basic security implications of modern computing environments.
- Understand the Federal, State and Local Cyber Defense partners/structures.
- Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk.
- Describe different types of attacks and their characteristics.
- Examine how the internet is used for cybercrime, cyber-stalking, and other abusive behaviors.
- Evaluate the effectiveness of applications of cybersecurity in preventing crime and abuse.

Required list of topics to be covered:

1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle
6. Data Security (in transmission, at rest, in processing)
7. Security Models
8. Access Control Models
9. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
10. Security Mechanisms (e.g., Identification/Authentication, Audit)
11. Malicious activity detection / forms of attack
12. Appropriate Countermeasures
13. Cybersecurity Principles
14. Endpoint protection
15. Storage Devices
16. System Architectures
17. Alternative environments (SCADA, real time systems, critical infrastructures)
18. Networks (Internet, LANs, wireless)
19. Software Security (secure coding principles)
20. Configuration Management
21. Vulnerability Scanning (core)
22. People and security (social engineering)
23. Physical and environmental security concerns
24. Internet Of Things (IOT)
25. The Adversary Model (resources, capabilities, intent, motivation and techniques)
26. Types of Attacks (and vulnerabilities that enable them)
27. Indicators of compromise
28. Attack surfaces
29. Covert Channels
30. Insider problem
31. Threat Information Sources (e.g., CERT)
32. Creation and operation of virtualization technology