Course number and name:	**CS 03351: Cyber Security: Fundamentals, Principles and Applications**
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:	(MATH 03160 Discrete Structures ***or*** MATH 03150 Discrete Mathematics) ***and*** CS 06205 Computer Organization
Type of Course:	☒ Required ☐ Elective ☐ Selected Elective

Educational objectives for the course:

1. Describe the fundamental concepts of the cyber security discipline and use to provide system security.
    - ABET (3) Communicate effectively in a variety of professional contexts.
2. Describe potential system attacks and the actors that might perform them.
    - ABET (3) Communicate effectively in a variety of professional contexts.
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
    - ABET (1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
4. Describe appropriate measures to be taken should a system compromise occur.
    - ABET (4) Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

5. Properly use the Vocabulary associated with cyber security.
    - ABET (3) Communicate effectively in a variety of professional contexts.
6. Define the principles of cybersecurity.
    - ABET (3) Communicate effectively in a variety of professional contexts.
7. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk.
    - ABET (3) Communicate effectively in a variety of professional contexts.
8. Describe the basic security implications of modern computing environments.
    - ABET (3) Communicate effectively in a variety of professional contexts.

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