Master of Science in Cybersecurity

Syllabus for CYB 701
IT and Operating Systems Security

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

This course introduces students to fundamental concepts of modern computing environments and their security implications. Students will explore information technology components including computer hardware, networks, and operating systems while developing practical knowledge of endpoint protection, vulnerability management, and security controls. Emphasis is placed on both technical understanding and security awareness.

Prerequisite(s)

None

Program Outcomes

This course addresses the following competencies and program outcomes of the Master of Science in Cybersecurity:

- Program Outcome 1: Foundational – Students will describe key principles of cybersecurity.

Course Outcomes

Upon completing this course, you will be able to do the following:

- Analyze modern computing infrastructure and security
- Assess the security implications of computing infrastructure
- Apply core cybersecurity concepts and controls to a computing environment

Course Requirements/Components

Computing Infrastructure and Security Fundamentals

- Hardware Components and System Architectures
- Operating Systems Fundamentals
- Storage Devices
- Alternative Computing Environments, IoT Infrastructure
- Cloud and Virtualization

Core Security Concepts and Controls

- Endpoint Protection
- Access Control Models
- Privileged vs. Non-privileged States
- Domain Separation

- Process Isolation, Resource Encapsulation
- Security Design Principles and Least Privilege

Network and System Security

- Network Fundamentals and Network Mapping
- Network Security Components
- VPNs and Firewalls
- Data Loss Prevention
- Intrusion Detection/Prevention Systems
- Vulnerability Scanning
- Configuration Management
- Patch Management and Software Security
- Incident Response
- Physical Security

Cybersecurity Partnerships and Human Factors

- Federal Cyber Defense Structures
- State and Local Partnerships
- Industry Partnerships
- Managed Services
- Social Engineering Fundamentals
- Human Factors in Security
- Physical and Environmental Security

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	90% or greater
A-	87% - < 90%
B+	83% - < 87%
B	80% - < 83%
B-	77% - < 80%
C+	73% - < 77%
C	70% - < 73%
C-	65% - < 70%
F	0 - < 65%

Assignments	Percentage
Discussions	20%
Assignments	40%
Quizzes	40%
Total	100%


Master of Science in Cybersecurity