Master of Science in Cybersecurity

Syllabus for CYB 765
Security Program Management

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 is an introduction to cybersecurity program management and compliance. Students will explore the development, implementation, and evaluation of security programs taking relevant legal and regulatory requirements into account. Topics include security policies, incident response, federal regulations, and emerging security challenges in today's digital landscape.

Prerequisite(s)

CYB 700 Fundamentals of Cybersecurity

Program Outcomes

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

- Program Outcome 3: Cybersecurity planning and management – Perform security risk analysis for an organization and develop system-specific security programs
- Program Outcome 4: Policy/Legal/Ethics/Compliance – Explain the role of policy, law, ethics in cybersecurity and ensure compliance with relevant organizational policies and regulatory frameworks.

Course Outcomes

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

- Develop and evaluate organizational security programs
- Analyze the core components of enterprise security management
- Interpret and apply legal and ethical responsibilities relevant to cybersecurity

Course Requirements/Components

Foundations of security program development

- Goals and objectives of security programs
- Metrics for program effectiveness
- Security baselines
- Security policies and procedures
- Best practices and frameworks

Enterprise security management

- Physical and personnel security
- System and data identification

- Configuration and patch management
- System documentation
- Incident response programs
- Disaster recovery planning

Regulatory compliance

- State, Federal, and International Laws and Standards
- Computer Security Act, Cybersecurity and Infrastructure Security Agency Act
- Sarbanes-Oxley
- HIPAA/FERPA
- USA PATRIOT Act
- Privacy regulations
- PCI DSS requirements
- Compliance

Legal and ethical considerations

- Legal disputes in cybersecurity
- Evidence handling
- Ethical considerations
- Data handling responsibilities
- Emerging security challenges

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%