Course number and name:	**CS 03506: Cybersecurity Management, Policy, and Risk**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Sally Tarabah
Text book, title, author, and year:	(optional textbook) *Developing Cybersecurity Programs and Policies*, 3rd edition by Omar Santos, 2019

Specific course information

Catalog description: This course covers cybersecurity planning and management, security risk analysis, policy, legal, ethics and compliance issues and security program management from a technical cybersecurity perspective.

Prerequisites: none

Type of Course: ☒ Required (MSCyb) ☐ Elective ☐ Selected Elective

Specific goals for the course:

1. At the conclusion of this course, you will have a basic understanding of:
   - Writing Effective Cybersecurity Policy
   - Planning and Management Cybersecurity Security Roles
   - Asset Management and Data Loss Prevention
   - Access Control Management
   - Physical and Environmental Security
   - Cyber Risk in the Cloud and IoT
   - Cybersecurity Incident Response
   - Risk Management and Methodologies, and Practices
   - Business Continuity Management and Disaster Recovery
   - Regulatory Compliance (including GLBA, HIPAA, PCI, GDPR, CCPA, etc.)
   - Legal Foundation of Cyber Law and Policy
   - Cyberethics – Morality in Cyberspace (Free Speech, Censorship, Intellectual Property, and Privacy Rights)

2. Upon completion of coursework, students will be able to produce a business cybersecurity protocol including business continuity, disaster recovery, and physical/environmental security components.

Required List of Topics to Be Covered:

1. Understanding cybersecurity policy organization, format, and styles
2. Cybersecurity framework
3. Governance and risk management
4. Asset management
5. Data loss prevention
6. Data privacy – GDPR and CCPA
7. Human resources security
8. Physical and environmental security
9. Access control management
10. Active directory fundamentals
11. Business Continuity and Disaster Recovery
12. Incident Response Plans
13. Legal foundation and regulatory compliance
14. Cyber ethics, free speech, censorship, and intellectual property