CYBERSECURITY (CYB)

CYB-1100 Foundations in Cybersecurity Management (4 semester hours)
Analyze and draft cybersecurity policies; create practical approaches to risk analysis; practice techniques to prevent intrusions and attacks that threaten organizational data; and participate in exercises in cryptography, ethical hacking, and crisis management.
Prerequisite(s): CSC-1700 or CSC-1010.

CYB-1810-9 Selected Topics in Cybersecurity (Variable semester hours)
This course will address a specific area of study in cybersecurity not already covered by other course offerings. Prerequisites vary by topic.

CYB-2100 Communicating, Problem Solving, and Leading in Cybersecurity (4 semester hours)
Make yourself more valuable to an employer by gaining and improving skills in communication and problem solving. Explore the field of cybersecurity by developing connections to your career aspirations, creating a professional social network presence, and using critical thinking to inform decisions. Improve and refine your skills in communication, critical thinking, quantitative reasoning, and team leadership. Hone your professional writing and oral communication skills to produce effective presentations and become proficient with current technology.

CYB-2810-9 Selected Topics in Cybersecurity (Variable semester hours)
This course will address a specific area of study in cybersecurity not already covered by other course offerings. Prerequisites vary by topic.

CYB-3100 Cybersecurity Governance (4 semester hours)
Examine important human aspects of cybersecurity, such as the motivations for cybercrimes, including hacker psychology and hacker culture. Explore the legal and regulatory environments related to local, state, national and international cybersecurity concerns. Formulate policy and conduct analysis for the prevention of intrusions, attacks, and threats to organizational data
Prerequisite(s): CYB-1100; CYB-2100.

CYB-3300 Risk Management and Organizational Resilience (4 semester hours)
Apply critical thinking and analysis to determine potential risks to the enterprise. Investigate the application of systems, tools, and concepts to minimize risk in an organization's cyberspace initiatives. Explore how to identify threats, conduct vulnerability assessments, and perform risk assessment and management. Examine system development and application assurance from a holistic viewpoint that spans the cyberspace landscapes. Gain an understanding of the value provided by regulatory, policy, and compliance guidelines in addition to pure technology options.
Prerequisite(s): CYB-1100; CYB-2100.

CYB-3500 Cybersecurity Program Development (4 semester hours)
Create a cybersecurity program using the enterprise as a framework. Examine the role of architectural methodology as part of the complete cybersecurity program. Consider the cyber threat landscape and the strategies related to incident response, awareness, and the mobile environment and its impact on government and industry. Explore identity theft, network security, cyber strategy development, and mobile device management.
Prerequisite(s): CSC-3200.

CYB-3600 Cryptography and Encryption (4 semester hours)
This course covers the techniques and methods used in modern cryptography to secure and protect data. Topics include private and public key encryption, hashing, digital signatures, authentication methods, ciphers, and strengths of cryptosystems. Programming is required.
Prerequisite(s): CSC-2150; MTH-3270.

CYB-3810-9 Selected Topics in Cybersecurity (Variable semester hours)
This course will address a specific area of study in cybersecurity not already covered by other course offerings. Prerequisites vary by topic.

CYB-4500 Cybersecurity Program Development (4 semester hours)
Create a cybersecurity program using the enterprise as a framework. Examine the role of architectural methodology as part of the complete cybersecurity program. Consider the cyber threat landscape and the strategies related to incident response, awareness, and the mobile environment and its impact on government and industry. Explore identity theft, network security, cyber strategy development, and mobile device management.
Prerequisite(s): CYB-3100 or CYB-3300.

CYB-4610 Ethical Hacking (4 semester hours)
Formerly CSC-4610. This course aims to provide knowledge and skills required to understand the mechanics behind hacking attacks, and develop appropriate safeguards. The course focuses on the code of conduct and ethics of attacking systems. The course also teaches the mindset of the criminal hacker and evolution of the hacker.
Prerequisite(s): CSC-3350.

CYB-4620 Digital Forensics (4 semester hours)
Formerly CSC4620. An introduction to the fundamental concepts behind the collection and analysis of the digital evidence left behind in a digital crime scene. Topics include the identification, preservation, collection, examination, analysis, and presentation of evidence for prosecution purposes. Discussion also covers the laws and ethics related to computer forensics and challenges in computer forensics.
Prerequisite(s): CSC-3350.

CYB-4810-9 Selected Topics in Cybersecurity (Variable semester hours)
This course will address a specific area of study in cybersecurity not already covered by other course offerings. Prerequisites vary by topic.

CYB-4940 Cybersecurity Internship (4 semester hours)
The purpose of the Cybersecurity Internship is to enable Aurora University students to acquire work experiences in the world of business or related-contexts. This experience is designed to expand on the learning experience and to integrate and reinforce skills and concepts learned in the classroom. The internship provides a practical experience in a structured employment environment. Students may repeat this course involving a different internship experience for a maximum of 12 semester hours. Letter grading applies. Permission of the instructor required.

CYB-4990 Capstone in Cybersecurity (4 semester hours)
Assume the role of a cybersecurity professional by examining current issues in cybersecurity management, including enterprise risk management, vulnerability assessment, threat analysis, crisis management, security architecture, security models, security policy development and implementation, security compliance, information privacy, identity management, incident response, disaster recovery, and business continuity planning, particularly in the health, banking, and finance sectors.
Prerequisite(s): CYB-3100; CYB-3300; CYB-3500.