Master of Science in Cybersecurity

Dr. Kevin Harris, Program Director

Program Mission

The mission of the Master of Science in Cybersecurity is to educate graduates to make a significant contribution, with a commitment toward moral purpose and productive work, within the information security community in support of individual, corporation, governmental services and organizational strategic goals.

Program Description

The Master of Science in Cybersecurity program is built to expand upon the undergraduate Cybersecurity program, while providing bachelor's degree prepared individuals the opportunity to gain additional knowledge, skill and experience, and establish competency in the field of Cybersecurity at the graduate level. The M.S. in Cybersecurity has earned specialized business accreditation from the Accreditation Council for Business Schools & Programs (ACBSP).

- Graduates will be prepared to contribute to and lead others in quickly evolving areas of Cybersecurity, including strategy, intelligence, and information assurance.
- The Cybersecurity program covers seven main categories of cyber operations, in alliance with The National Cybersecurity Workforce Framework. Graduates will be prepared to conduct the following Cybersecurity roles in organizations: (1) securely provision, (2) operate and maintain, (3) protect and defend, (4) investigate, (5) collect and operate, (6) analyze, and (7) oversight and development.
- Graduates will focus strongly on the oversight and development of Cybersecurity initiatives preparing them for a variety of managerial and leadership careers in the rapidly growing industry of Cybersecurity.
- The National Initiative for Cybersecurity Careers and Studies indicates immediate demand for this profession. Graduates can anticipate employment in corporate, government and military organizations.

Program Learning Outcomes

The Master of Science in Cybersecurity will provide leaders of public and private organizations with the ability to:

1. Evaluate and defend the mission of an organization requiring security defense by analyzing the needs and costs of creating security related programs and strategies.
2. Analyze the demands of systems security and practiced methodologies for protecting data integrity and confidentiality through ethical practices.
3. Synthesize a variety of challenging policy, legal, and technological concepts in relation to cybersecurity.
4. Evaluate security theories, apply experiential lessons learned, evaluate

new research and generate new research and security models for organization's who require security related and information management strategies.

What You Will Study

Degree Requirements

The graduate program consists of 30 credit hours.

Master of Science in Cybersecurity – Core Curriculum	
Course	**Credits**
CYBR 610: Cyber Operations Management	3
CYBR 615: Strategic Cyber Intelligence	3
CYBR 620: Legal Issues in Cybersecurity	3
CYBR 625: Cyber Psychology	3
CYBR 630: Offensive and Defensive Strategies	3
CYBR 635: Security and Information Data Analytics	3
CYBR 660: Capstone: Practical Applications in Security	3
Total Credits	**21**

Master of Science in Cybersecurity Concentrations

Cybersecurity Strategy	
Course	**Credits**
CYBR 640: Strategic Investments in Information Security	3
CYBR 645: Enterprise Infrastructure Planning & Safeguarding	3
CYBR 650: Cybersecurity Policy Implementation	3
Total Degree Credits	**30**
Total Certificate Credits	**12**
Cyber Intelligence	
Course	**Credits**
CYBR 710: Open Source Intelligence	3
CYBR 715: Social Media Intelligence	3
CYBR 720: Information Operations	3
Total Degree Credits	**30**
Total Certificate Credits	**12**
Information Assurance	
Course	**Credits**
CYBR 810 Information Assurance & Risk Management	3
CYBR 815: Security Governance Frameworks	3
CYBR 820: Security & Regulatory Compliance	3
Total Degree Credits	**30**
Total Certificate Credits	**12**

Transfer Credit

Students enrolled in the MSCS program, or certificate program, must take a minimum of 21 total credit hours from the University of Charleston, and may transfer a maximum of

9 credit hours from a regionally accredited university (subject to approval by the Program Director). Three of the required 21 credit hours must include the CYBR 660 capstone course.

Admission Requirements

Applicants to the program must have completed a Bachelors degree in Business, Information Technology, or a related Information Sciences field at a regionally accredited institution of higher education. Technological literacy gained from prior coursework is imperative for success in the program. No entrance examinations are required, as proof of prior performance and recommendations are used as entrance assessments.

Satisfactory Academic Progress

A final grade of C, or better, is required for the CYBR 660 capstone course to complete the degree requirements.

Level I Probation – Students who obtain a term GPA less than 3.0 must meet with the program director to discuss plans for better performance. If appointments are not made or kept, the student may not be permitted to register for subsequent semesters. Students who obtain a term GPA less than 3.0 will be limited to a maximum of 6 credits in the following semester.

Level II Probation– Students who obtain a term GPA less than 3.0 a second time are placed on Level II probation. Students on Level II Probation may be required to repeat a course(s) and complete remedial work under the supervision of faculty members. Students may only be on Level II Probation for one semester over their time at the University. Students will meet with program director to discuss plans for better performance. If appointments are not made or kept, the student may not be permitted to register for subsequent semesters.

Failure to obtain a cumulative GPA of 3.0 or higher while on Level II Probation or demonstrate satisfactory progression per plans for better performance will result in dismissal from the Program. The final decision on dismissal will be made by the Program Director and Associate Dean considering the following factors: significant improvement of the term GPA and an improvement in the cumulative GPA. Students must have a minimum cumulative GPA of 3.0 to graduate from the Master of Science in Cybersecurity program from the University of Charleston.

Should the student wish to appeal his/her dismissal, he/she must do so within fourteen calendar days from the date of receipt of the dismissal letter, unless the Program Director grants a delay due to extenuating circumstances. Students can petition for readmission one year after dismissal but not before that time.