CYBERSECURITY / MASTER OF SCIENCE

The Master of Science in Cybersecurity (MSCY) program provides students with well-rounded expertise in this inherently interdisciplinary field. Cybersecurity is a problem having both human and technological causes and solutions. The design of the program's curriculum reflects these dual emphases.

Students will learn how to create and use technologies to protect organizations, people, and their data. Courses address vulnerabilities and remedies in networks, operating systems, servers, services, file systems, and software. Students learn how to protect data in transit and at rest through encryption and authentication using a variety of tools and technologies. Ultimately, these tools are used by people who may be serving an organization, and that organization must employ more than just technology to keep their systems secure. Organizations must institute effective policies and strategies for managing and monitoring risk and assessing security in an ongoing way. Accordingly, the curriculum includes courses that address these topics, too.

To accommodate the needs of working professionals, the program is structured for part-time students with courses offered in the evenings. All courses are offered in an eight-week format both online and on campus.

Requirements

Degree Offered: Master of Science
Total Credit Hours: 33-45

Degree Requirements

Code	Title	Hours
Foundation Courses [1]		
CPSC 50000	Computer Organization	3
CPSC 50100	Programming Fundamentals	3
CPSC 50500	Communications and Networking	3
CPSC 51500	Operating Systems	3
Core Courses		
CPSC 50600	Cyber Security Essentials [2]	3
CPSC 50700	Advanced Cyber Security	3
CPSC 52000	Network Security Essentials	3
CPSC 52500	Encryption and Authentication [2]	3
CPSC 59100	Cybersecurity Project	3
INSY 53000	Legal and Ethical Issues in Information Security	3
Business and Management Courses		
Select two of the following:		6
INSY 55000	Operations and Organization Security	
INSY 55100	Information Security Strategies and Risk Management	
INSY 55200	IT Governance and Compliance	
INSY 55600	Disaster Recovery and Business Continuity Planning	
Electives		
Select three of the following: [3]		9
INSY 55000	Operations and Organization Security	
INSY 55100	Information Security Strategies and Risk Management	
INSY 55200	IT Governance and Compliance	
INSY 55600	Disaster Recovery and Business Continuity Planning	
CPSC 56000	Securing Operating Systems	
CPSC 66500	Application Security	
CPSC 67000	Cloud and Virtualization Security	
CPSC 67300	Digital Forensics	
CPSC 67500	Network Forensics	
CPSC 67600	Mobile Device Forensics	
CPSC 68000	Advanced Network Security	
CPSC 68500	Enterprise Network Security	
Total Hours		**45**

1. Foundation courses are additional courses required by students without prior coursework in computer science. A given foundation course may be waived if the student has completed a similar course or shows a professional experience that satisfies the coursework.
2. If equivalents of CPSC 50600 Cyber Security Essentials or CPSC 52500 Encryption and Authentication have been taken at the undergraduate (300-level and above) or graduate level, students may substitute any of the elective courses below for them (not reducing required credit hours).
3. Not used to fulfill the Business and Management Courses requirement

Additional Admission Requirements Full Admission

To be accepted for admission into the program, a student must present the following credentials:

1. A baccalaureate degree from a regionally-accredited institution of higher education.
2. A minimum undergraduate GPA of 3.0 on a 4.0 scale.
3. An application for graduate admission, accompanied by an application fee.
4. Professional résumé.
5. Official transcripts from all institutions of higher education attended.
6. A two-page statement of purpose.
7. Two letters of recommendation.

Please note: International students are required to have a TOEFL test score greater than 550 (computer-based 213; internet-based 79).

Provisional Admission

Under certain circumstances, students who do not meet one or more of the requirements for full admission may be admitted to the program on a provisional basis. Provisional admission is most commonly offered to applicants who earned an undergraduate GPA less than 3.0 (but greater than 2.5). Students granted provisional status will be considered for full admission by the Graduate Program Director in consultation with the Graduate Council of the College of Aviation, Science, and Technology only after they have attempted nine credit hours in the program and earned a GPA of 3.0 out of 4.0. Provisionally-admitted students who have not attained the minimum GPA of 3.0 after attempting nine credit hours of MSCY coursework will be dismissed from the program.

Student-At-Large

A student-at-large is not a degree candidate. In order to be admitted as a student-at-large, the applicant must submit official documentation of a baccalaureate degree from a regionally-accredited institution of higher education and complete a modified application form. The decision to admit an at-large student to graduate courses belongs to the Graduate Program Director, whose decision is based on an evaluation of the applicant's undergraduate coursework and possibly an interview. However, should the student decide to apply for full admission status at a later time, but within five years of course completion, only a maximum of nine semester hours of graduate coursework completed as a student-at-large can be applied toward an advanced degree, and only courses with grades of B or better will count toward the degree.

Foundation Coursework

Students who lack prior coursework in computer science or management information systems from an accredited collegiate institution are required to take up to four foundation courses in the major to gain background in computer programming, computer organization, networks, and operating systems. The determination of whether a student is required to take one or more foundation courses will be made during the application review process by the Graduate Program Director. The Graduate Program Director will evaluate the applicant's prior academic transcripts, looking for courses in computer programming, computer organization, networks, and operating systems. If the transcripts provide evidence of academic credit in these areas from a regionally-accredited institution of higher education, the student will not be required to take the corresponding foundation course. The foundation courses are designed to provide students who lack prior academic coursework in the fundamentals of Computer Science the concepts they need to appreciate fully the technical aspects of cybersecurity.

Transfer of Graduate Credit

A student entering the Master of Science in Cybersecurity program with appropriate prior graduate coursework in the field may have a maximum of nine credit hours beyond the foundation courses applied to the MSCY degree. Course credits eligible for transfer consideration must meet the following criteria:

1. All transfer credit must have been earned prior to matriculation in the MSCY program.
2. The coursework must have been completed at a regionally-accredited graduate school.
3. Only courses with a minimum grade of B are acceptable.
4. The coursework must have an equivalent course in the MSCY curriculum.
5. Courses from outside the United States will be considered if they are evaluated as graduate level by the Office of Admission or the Commission on Accreditation of the American Council on Education.
6. Credit for prior learning is not awarded for graduate courses.

International Students

International students are required to meet all the admission requirements for full or provisional admission and also the admission requirements specified in the Admission Policies section (https://catalog.lewisu.edu/graduate/general-information/admission-policies/) of this Catalog entitled "Entering International Students."