Cybersecurity MS, Information Systems Emphasis

Students must meet all general University of Missouri-St. Louis Graduate School admission and degree requirements.

Students must choose one of the following emphasis areas at the time of application for admission:

1. Information Systems Emphasis or
2. Computer Science Emphasis

Degree requirements vary depending on the chosen emphasis area.

Applicants must meet the general graduate admission requirements of the Graduate School, described in the UMSL catalog. Students are considered for admission to the graduate program in Cybersecurity only after they have formally applied for admission through the Graduate School. Applications may be completed on-line.

Additional emphasis specific requirements are listed below.

Admission Requirements

In addition to Graduate School admission requirements, the following requirements apply.

Applicants must have an undergraduate degree with a minimum cumulative GPA of 3.0. Students whose GPAs are between 2.75 and 2.9 may be admitted under a restricted status within the terms specified by the Graduate School.

Prior to entry, students must demonstrate competence in the following areas (through prior course work or professional experience) or take coursework at UMSL to fulfill the entry requirements.

- Business Statistics (similar to undergraduate course SCMA 3300). Students without a background in statistics could take SCMA 5300 as a graduate student to fulfill this requirement.
- At least one semester of computer programming coursework or application development work experience (similar to undergraduate courses INFSYS 3806 or INFSYS 3844). Students without programming background can take either INFSYS 6805 or INFSYS 6806 as a graduate student to fulfill this requirement.

Entrance examinations

- The Graduate Management Admission Test (GMAT) is not required for admission. However, it may be used by students when their overall GPA is below 3.0 to strengthen their application.
- International students are required to document English proficiency by providing scores from an internationally accepted standardized examination before a decision is made on admission

Coursework

Candidates for the M.S. in Cybersecurity with Information Systems Emphasis must complete 30 credit hours of graduate coursework subject to Graduate School requirements.

Required Courses

INFSYS 6820	Systems and IT Infrastructure	3
INFSYS 6828	Principles of Information Security	3
INFSYS 6836	Management of Data Networks and Security	3
INFSYS 6858	Advanced Cybersecurity Concepts	3
INFSYS 6864	Applied Cryptography for Business Applications	3
INFSYS 6868	Software Assurance	3
INFSYS 6878	Management of Information Security	3
INFSYS 6888	Capstone in Information Security	3
Electives (select two from following)		**6**
CMP SCI 5732	Cryptography for Computer Security	
CMP SCI 5750	Cloud Computing	
INFSYS 5890	Graduate Internship in Information Systems	
INFSYS 5899	Individual Research in Information Systems [1]	
INFSYS 6818	Management of Software Testing	
INFSYS 6847	Project Management	
INFSYS 6860	Advanced Data Integration	
INFSYS 6862	Artificial Intelligence Applications for Business and Cybersecurity	
INFSYS 6891	Seminar in Information Systems [1]	
MGMT 5600	Managing and Leading in Organizations	
Other electives upon approval of Information Systems department chair		
Total Hours		**30**

[1] Topic must be approved by Information Systems department chair

Learning Outcomes

Upon completion of the program, graduates will be able to:

- Apply fundamental security principles and formal security models to solve many complex problems in cybersecurity.
- Develop, maintain, and update an organization's information security policies to meet security and compliance requirements.
- Select and execute appropriate security mechanisms to implement security policies of an organization.
- Evaluate and maintain information systems for secure and reliable operations by employing appropriate risk management strategies.
- Communicate cybersecurity issues effectively to a range of audiences.
- Function effectively as a leader or member of a team engaged in activities appropriate to the cybersecurity discipline.