

CYBERSECURITY, M.S.

The curriculum for the Master of Science in Cybersecurity teaches students to apply information security principles to analyze, detect, and mitigate vulnerabilities and intrusions to cyberinfrastructure. Students also gain a deeper appreciation and understanding of the social, policy, ethical and legal aspects of security and privacy. Graduates are prepared to manage and lead cyber teams and programs in roles ranging from government cybersecurity analyst to data security consultant. A unique aspect of the program is the ability to earn a graduate certificate that complements a master's degree, often without taking additional credits. This enables students to tailor the program to their specific interests.

Careers

The master's degree in cybersecurity prepares you to manage and lead cyber teams and programs. Graduates of the cybersecurity program have the foundation necessary to succeed as network and computer systems administrators, government cybersecurity analysts, computer systems analysts, information security analysts, computer and information systems managers, and data security consultants.

Admission Requirements

- An undergraduate degree from an accredited institution
- Most successful applicants have an undergraduate grade point average of 3.0 or better
- Two or more years of work experience is recommended (full-time or part-time employment, internships, co-ops and similar experiences)

Application Requirements

- Application form and fee
- Transcript(s)
- Three external reference evaluations
- Résumé
- An essay of about 500 words that describes:
 - What attracted you to this program?
 - How will a master's degree in this field benefit you in your present or future career?

Requirements for International Students

All admission policies and requirements for domestic students apply to international students along with the following:

- Demonstrate English language proficiency. Some examples of demonstrated English language proficiency include minimum score requirements for the following standardized tests:
 - Paper-based TOEFL: 550
 - Internet-based TOEFL: 80
 - IELTS: 6.5
 - PTE: 54
- Academic records, in English translation, of students who have undertaken postsecondary studies outside the United States must include the courses taken and/or lectures attended, practical laboratory work, the maximum and minimum grades attainable, the grades earned or the results of all end-of-term examinations, and any honors or degrees received. WES and ECE transcripts are accepted.

- Proof of financial support, which must include:
 - A letter of financial support from the person(s) or sponsoring agency funding the time at Saint Louis University
 - A letter from the sponsor's bank verifying that the funds are available and will be for the duration of study at the University

Application and Assistantship Deadlines

Students should apply for the fall semester by July 1 and for the spring semester by Nov. 1.

The application deadlines for international students are: May 15 (fall), October 1 (spring) and February 1 (summer).

Students seeking assistantships should apply by Feb. 1.

Review Process

Application decisions are made per guidelines and a review process established by the department, school or college.

Scholarships and Financial Aid

For priority consideration for graduate assistantship, applicants should complete their applications by February 1.

For more information, visit the Office of Student Financial Services online at <http://www.slu.edu/financial-aid>.

Learning Outcomes

1. Graduates will be able to apply program-specific knowledge to address practical problems using an ethical, evidence-based framework.
2. Graduates will be able to utilize argumentation skills appropriate for a given problem or context.
3. Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.
4. Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Requirements

Code	Title	Credits
Graduate Core Courses		
Graduate core requirements (p. 2)		9
Foundation Courses		
CYBR 5000	Cybersecurity Principles	3
CYBR 5010	Networking Concepts	3
CYBR 5020	Data Administration	3
CYBR 5030	Cyber Threats and Defense	3
Electives		
Select three of the following:		9
CYBR 5210	Digital Investigations	
CYBR 5220	Incident Response and Mitigation	
CYBR 5230	Intrusion Detection and Analysis	
CYBR 5240	Cloud Security	
Applied Research Project		
CYBR 5961	Cybersecurity Masters Research Project I	1
CYBR 5962	Cybersecurity Masters Research Project II	1
CYBR 5963	Cybersecurity Masters Research Project III	1
Total Credits		33

Continuation Standards

Students must maintain a cumulative grade point average (GPA) of 3.00 in all graduate/professional courses.

Graduate Core Courses

		Credits
ORLD 5050	Ethical, Evidence-Based Decision Making	3
AA 5221	Applied Analytics & Methods I	3
INTL5961-5963	Strategic Intelligence Master's Research Project (MRP)	3
Total Credits		9

Contact Information

Learn more and apply for admission at slu.edu/globalgrad.
Contact us at globalgrad@slu.edu with any questions.