CYBERSECURITY, POST-BACCALAUREATE CERTIFICATE

Gain the skills and preparation you need to succeed as a competitive professional in the field of cybersecurity through the graduate certificate in cybersecurity at Saint Louis University's School for Professional Studies.

If you complete the certificate, you also have the option of applying to the Master of Science in Cybersecurity (https://catalog.slu.edu/colleges-schools/professional-studies/cybersecurity-ms/) program and, if accepted, have all of the certificate credits count toward the master's degree.

Curriculum Overview

As part of the School for Professional Studies, this 12-credit, fully online program offers technology-driven professionals like you a flexible option to meet your personal career goals. If you have obtained an undergraduate degree or higher, you may pursue a stand-alone certificate. All courses are offered in eight-week terms through SLU Online, making advanced education more accessible for working professionals.

The curriculum for SLU's cybersecurity certificate is designed to help you learn to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions to your organization's cyberinfrastructure. With coursework focused on learning cybersecurity principles, administration of data, identification of cyber threats, and ways to defend against these threats, you will be more prepared to lead cyber teams and programs in roles ranging from government cybersecurity analyst to data security consultant.

Careers

SLU's post-baccalaureate certificate 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, and computer and information systems managers.

Admission Requirements

- Completed application.
- Official transcript from a degree-granting institution.
- Most successful applicants have an undergraduate grade point average of 3.0 or better.
- At least two years of work experience is recommended (includes full-time and part-time employment, internships, co-ops and similar experiences).
- Statement of professional goals (approximately 500 words suggested) articulating what attracted you to this program, and how a master's degree in this field will benefit you in your present or future career.
- Resume or curriculum vitae.

Requirements for International Students

Along with the general admission requirements above, the following must be provided by prospective international students:

- Demonstration of 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, for postsecondary studies outside the United States. These 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.

Application and Assistantship Deadlines

Students should apply for the fall semester by August 6 and the spring semester by January 7.

Review Process

Applications are reviewed by program directors.

Apply Now (http://www.slu.edu/apply.php)

Scholarships and Financial Aid

For priority consideration for graduate assistantship, apply by Feb. 1.

For more information, visit the student financial services office online at http://finaid.slu.edu.

Learning Outcomes

1. Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.
2. Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Requirements

Code	Title	Credits
CYBR 5000	Cybersecurity Principles	3
CYBR 5010	Networking Concepts	3
CYBR 5020	Data Administration	3
CYBR 5030	Cyber Threats and Defense	3
Total Credits		**12**

Continuation Standards

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

Roadmap

Roadmaps are recommended semester-by-semester plans of study for programs and assume full-time enrollment unless otherwise noted.

Courses and milestones designated as critical (marked with !) must be completed in the semester listed to ensure a timely graduation. Transfer credit may change the roadmap.

This roadmap should not be used in the place of regular academic advising appointments. All students are encouraged to meet with their advisor/mentor each semester. Requirements, course availability and sequencing are subject to change.

Course	Title	Credits
Year One		
Fall		
Fall 1		
CYBR 5000	Cybersecurity Principles	3
Fall 2		
CYBR 5010	Networking Concepts	3
	Credits	**6**
Spring		
Spring 1		
CYBR 5020	Data Administration	3
Spring 2		
CYBR 5030	Cyber Threats and Defense	3
	Credits	**6**
	Total Credits	**12**

Contact Us

Apply for Admission (https://www.slu.edu/online/becoming-a-student/apply.php)

For additional admission questions, please call 314-526-2825 or email sps@slu.edu.