CYBERSECURITY, M.S.

Offered in a completely online format, you can earn a graduate certificate that complements your master's degree, often without taking additional credits. This allows you to tailor the program to your specific interests.

Curriculum Overview

The Master of Science in Cybersecurity program at Saint Louis University is professionally oriented, for those interested in careers in private-sector cybersecurity. The program is ideal for students who seek both a strong foundation and detailed technical knowledge in security, privacy and intelligence. You will learn how to apply that knowledge to information systems, networks and software and gain a deeper appreciation of the social, policy, ethical and legal aspects of security and privacy.

Designed for working professionals, our program is flexible, and courses are offered in a 8-week format — allowing you to stay focused on your career as you earn your degree. Our online courses allow students to access course content 24/7 without having a specific class meeting time. Using the latest video capture and discussion board technology, students are required to meet and collaborate with instructors and classmates in an asynchronous online format. To ensure individual attention and mentoring by our distinguished faculty, we typically limit courses sections to 20 students.

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

- **Minimum undergraduate GPA: 3.00**
- Applicant must be employed on at least a part-time basis (20 hours or more per week) and have at least three years of work experience
- Completed coursework in the following areas:
  - At least one course in information systems/technology or a programming language.
  - At least one basic statistics or research methods course.
  - Skills in using business productivity software and understanding of basic level software installation and troubleshooting procedures.

Applicants who have a GPA that is less than 3.0 will be considered on a case-by-case basis, by considering the strength of the remaining components of their application.

Students missing any of the above prerequisites will be permitted to fulfill them through the School for Professional Studies prior to acceptance into the program.

Application Requirements

- Application form and fee
- Transcript(s)
- Three recommendations submitted using the Applicant Evaluation Form.
- Résumé

- A 500-word personal statement articulating why a master’s degree is needed within present or future career and how the program will help meet that need.

Requirements for International Students

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

- Demonstrate English Language Proficiency (http://catalog.slu.edu/academic-policies/office-admission/graduate/english-language-proficiency)
- Proof of financial support 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 so for the duration of study at the University
- 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.

Application and Assistantship Deadlines

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

To be considered for an assistantship, apply by Feb. 1.

Review Process

Applications are reviewed by a committee of School for Professional Studies faculty members.

Scholarships and Financial Aid

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

Learning Outcomes

1. Graduates will be able to assess evidence to draw reasoned, ethical conclusions.
2. Graduates will be able to apply leadership competencies appropriate for a given situation or context.
3. Graduates will be able to articulate arguments or explanations to both a disciplinary or professional audience and to a general audience, in both oral and written forms.
4. Graduates will be able to construct and implement networks and data management systems that protect intellectual property using cybersecurity principles.
5. Graduates will be able to apply information security principles to analyze, detect and mitigate vulnerabilities and intrusions.

Requirements

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Graduate Core Courses</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Graduate core requirements (p. 2)</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td><strong>Foundation Courses</strong></td>
<td></td>
</tr>
<tr>
<td>CYBR 5000</td>
<td>Cybersecurity Principles</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 5010</td>
<td>Networking Concepts</td>
<td>3</td>
</tr>
</tbody>
</table>
Saint Louis University Academic Catalog 2018-2019

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 5020</td>
<td>Data Administration</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 5030</td>
<td>Cyber Threats and Defense</td>
<td>3</td>
</tr>
</tbody>
</table>

**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 36

**Continuation Standards**

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

**Graduate Core Courses**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORLD 5010</td>
<td>Contemporary Organizational Leadership</td>
<td>3</td>
</tr>
<tr>
<td>ORLD 5050</td>
<td>Ethical, Evidence-Based Decision Making</td>
<td>3</td>
</tr>
<tr>
<td>AA 5221</td>
<td>Applied Analytics &amp; Methods I</td>
<td>3</td>
</tr>
<tr>
<td>AA 5222</td>
<td>Applied Analytics &amp; Methods II: Survey Approaches</td>
<td>3</td>
</tr>
<tr>
<td>or AA 5223</td>
<td>Applied Analytics &amp; Methods II: Experimental Approaches</td>
<td></td>
</tr>
</tbody>
</table>

Total Credits 12

**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.

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year One</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall 1</td>
<td>CYBR 5000  Cybersecurity Principles</td>
<td>3</td>
</tr>
<tr>
<td>Fall 2</td>
<td>ORLD 5050  Ethical, Evidence-Based Decision Making</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Credits 6

| Year Two   |                                            |         |
| Fall       |                                            |         |
| Fall 1     | CYBR 5010  Networking Concepts             | 3       |
| Fall 2     | CYBR 5030  Cyber Threats and Defense       | 3       |
| CYBR 5962  | Cybersecurity Masters Research Project II  | 1       |

Total Credits 7

| Year Three  |                                            |         |
| Spring      |                                            |         |
| Spring 1    | CYBR 5230  Intrusion Detection and Analysis | 3       |
| Spring 2    | CYBR 5963  Cybersecurity Masters Research Project III | 1 |

Total Credits 4

**Course Title**

- ORLD 5000  Organizational Dynamics 3
- CYBR 5210  Digital Investigations 3
- CYBR 5220  Incident Response and Mitigation 3
- CYBR 5961  Cybersecurity Masters Research Project I 1
- CYBR 5962  Cybersecurity Masters Research Project II 1
- CYBR 5963  Cybersecurity Masters Research Project III 1
- AA 5222  Applied Analytics & Methods II: Survey Approaches 3
- CYBR 5961  Cybersecurity Masters Research Project I 1
- CYBR 5962  Cybersecurity Masters Research Project II 1
- CYBR 5963  Cybersecurity Masters Research Project III 1
- AA 5221  Applied Analytics & Methods I 3
- CYBR 5961  Cybersecurity Masters Research Project I 1
- CYBR 5962  Cybersecurity Masters Research Project II 1
- CYBR 5963  Cybersecurity Masters Research Project III 1
- AA 5222  Applied Analytics & Methods II: Survey Approaches 3
- CYBR 5961  Cybersecurity Masters Research Project I 1
- CYBR 5962  Cybersecurity Masters Research Project II 1
- CYBR 5963  Cybersecurity Masters Research Project III 1
- AA 5221  Applied Analytics & Methods I 3