Cybersecurity

Saint Louis University is a world-class Catholic, Jesuit institution educating nearly 13,000 students on two dynamic, urban campuses - in St. Louis, Missouri, and Madrid, Spain. Founded in 1818, the University is now celebrating its bicentennial.

With a legacy of innovative academics and research, compassionate health care and faithful service, Saint Louis University attracts a diverse community of scholars who push intellectual boundaries in pursuit of creative, meaningful ways to impact the world, striving to serve a higher purpose and seek a greater good.

OVERVIEW

Saint Louis University’s online Masters in Cybersecurity prepares students for both corporate and public cybersecurity related positions, and teaches them the skills necessary to deal with organized and sophisticated cyber-attacks.

Offered in a completely online format, the program is professionally oriented, for those interested in careers in private sector cybersecurity. Designed for working professionals, our program is flexible and offered in 8-week modules – allowing you to stay focused on your career as you are earning your degree. To ensure individual attention and mentoring by our distinguished faculty, we typically limit courses sections to 20 students.

M.S.: The goal of this program is to prepare students who seek both a strong foundation and detailed technical knowledge in security, privacy, and intelligence applied to information systems, networks, and software as well as an appreciation of the social, policy, ethical and legal aspects of security and privacy.

The program strives to seek a balance between the theoretical and deep technical skills of cybersecurity. The program is suitable for students who have received a baccalaureate degree in computer science or a related field, and have a desire to join the cybersecurity community and workforce. The program will prepare our graduates to face the futuristic security related challenges emerging from our internet connected world, the rapid adoption of mobile devices, and the ever increasing role of cybersecurity in our daily life.

As a student in our program, you will join a community of academics and practitioners from around the world, giving you the opportunity to learn from and network with your peers. Our students represent a wide range of academic and professional backgrounds, including, cybersecurity, emergency management, analytics, and military and defense.

A unique aspect of the program is the ability to earn a graduate certificate that complements your Master’s degree, often without taking additional credit hours. This allows you to tailor the program to your specific interests.

Concentrations and certificate options (up to 9 hours in lieu of electives)

The Master of Science in cybersecurity program offers stackable graduate certificate options that enable you to focus your studies and gain an additional academic credential upon graduation. Students accepted for the M.S.in cybersecurity may simultaneously enroll in one of the following graduate certificates:

- Applied analytics
- Organizational leadership
- Organizational development
- Ethical based decision making

APPLICATION REQUIREMENTS

- Transcript(s) from all previous academic coursework
- Résumé
- Personal statement
- Three references must complete an applicant assessment

ADMISSION CRITERIA

In reviewing an application, previous academic performance in college-level coursework is examined holistically. All applications are considered on an individual basis with a balanced approach.

- Undergraduate GPA above 3.0 (students with less than a 3.0 may be provisionally admitted)
- Three years of work experience
- Coursework in the following areas:
  - At least one basic statistics or research methods course
  - At least one course in information systems/technology/programming

Note: Applicants who have a GPA less than 3.0 will be considered on a case-by-case basis. Students missing any of the prerequisite coursework will be permitted to fulfill those through SPS or an accredited postsecondary academic institution prior to acceptance into the program.
SAINT LOUIS UNIVERSITY
GRADUATE EDUCATION

Cybersecurity
+ School for Professional Studies

FACULTY
John P. Buerck, Ph.D.
Matthew Grawitch, Ph.D.
Keith Hacke, M.S.
Mark Henderson, M.S.
Srikanth Mudigonda, Ph.D.
Shannon Parker, M.B.A.
Ann Rohrer, Ph.D.
Tim Toennies, M.S.
Steve Winton, Ph.D.

CURRICULUM
To 36-hour Master of Science in cybersecurity requires the following courses:
Professional studies core (12 hours):
  • AA 5221: Applied Analytics and Methods I
  • AA 5222: Applied Analytics and Methods II: Survey Approaches -or-
  • AA 5223: Applied Analytics and Methods II: Experimental Approaches
  • ORLD 5050: Ethical, Evidence-Based Decision Making
  • ORLD 5010: Contemporary Org Leadership
Cybersecurity Core (12 Hours):
  • CYBR 5000 Cybersecurity Principles
  • CYBR 5010 Networking Concepts
  • CYBR 5020 Data Administration
  • CYBR 5030 Cyber Threats and Defense
Applied Research Project (3 Hours)
  • CYBR 5961-5963: Cyber Masters Research Project (MRP)
Electives (choose 9 Hours)
  • CYBR 5210 Digital Investigations
  • CYBR 5220 Incident Response and Mitigation
  • CYBR 5230 Intrusion Detection and Analysis
  • CYBR 5240 Cloud Security
Approved electives from other disciplines may also be considered.

Transfer Credit Policy
The M.S. in cybersecurity may accept a maximum of six semester credits of graduate-level classes, provided the credits are: a) from a regionally accredited institution, b) earned a grade of “B” or higher, c) relevant to the degree being sought. The director of the program and the dean must approve all requests for transfer credits and may set additional transfer requirements.