CYBERSECURITY (MS)

Program Directors: Jeffrey McConnell, PhD (/jmconnel@canisius.edu) and Jeffrey Spaulding, PhD (/jspauldi6@canisius.edu)

The M.S. in Cybersecurity program is designed to train cybersecurity professionals to meet the needs of business, industry, educational institutions, and government agencies locally and nation-wide. The program provides a cutting-edge curriculum that prepares graduates to succeed as a cybersecurity professional or researcher.

The Cybersecurity MS is designed as a full-time (with a part-time option), face-to-face program. Students without computer science background may take a set of courses as preparatory that would otherwise be waived for those with the applicable undergraduate courses. The program is in line with curricular recommendations from the ACM Cybersecurity Curricula and the NSA’s Center of Academic Excellence (CAE) in Cyber Defense.

Admissions Requirements

- Students from any undergraduate major are welcome to apply, as long as they have acquired a bachelor’s degree prior to the start of classes.
- Cumulative GPA of 2.8 or higher.
- Successful completion of a college-level Calculus 1 course (comparable to MAT 111 or MAT 11S at Canisius).
- Students may apply at any time. We have rolling admissions.
- Student preparation and background are used to determine if some introductory courses may be waived.

Materials to be Submitted

- Free Online Application (https://www.canisius.edu/admissions/apply-canisius/), with essay
- An official transcript from each college attended
- Official GRE or GMAT score (optional)
- Resumé (optional)
- One or two Letters of Recommendations (optional)

Policies

Academic Standing

The Cybersecurity program follows the College of Arts and Sciences on students’ academic standing. (http://catalog.canisius.edu/graduate/academics/academic-policies/#academicstandingtext)

Matriculation and Continued Program Enrollment

The Cybersecurity program follows the Canisius College policy for matriculated students (http://catalog.canisius.edu/graduate/admission-matriculation/#Matriculation) that expects students to maintain a continuous program of academic work.

Registration and Credit Hours

Cybersecurity students must be registered for at least 4.5 credits per semester to maintain eligibility for financial aid (if they are eligible). A full load is at least 9 credit hours. No student may register for more than 12 credit hours in any semester.

Curriculum

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 501</td>
<td>Introduction to Programming for Data Analytics</td>
<td>3</td>
</tr>
<tr>
<td>CSC 502</td>
<td>Data Structures and Algorithms</td>
<td>3</td>
</tr>
<tr>
<td>MAT 591</td>
<td>Discrete Mathematics</td>
<td>3</td>
</tr>
<tr>
<td>CSC 530</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
</tr>
<tr>
<td>CYB 500</td>
<td>Cybersecurity Principles and Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 510</td>
<td>Cybersecurity Policies, Ethics, and Law</td>
<td>3</td>
</tr>
<tr>
<td>CYB 520</td>
<td>Ethical Hacking and Penetration Testing and Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 540</td>
<td>Network and Internet Security and Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 600</td>
<td>Secure Software Engineering and Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 610</td>
<td>Cybersecurity Project</td>
<td>3</td>
</tr>
<tr>
<td>CYB 620</td>
<td>Applied Cryptography and Lab</td>
<td>3</td>
</tr>
<tr>
<td>DAT 513</td>
<td>Database Management and Lab</td>
<td>3</td>
</tr>
<tr>
<td>Choose one of the following:</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CYB 599</td>
<td>Cybersecurity Special Topics and Lab</td>
<td></td>
</tr>
<tr>
<td>CYB 611</td>
<td>Cybersecurity Thesis</td>
<td></td>
</tr>
<tr>
<td>CYB 697</td>
<td>Cybersecurity Internship</td>
<td></td>
</tr>
</tbody>
</table>

Total Credits 39

For course descriptions, click on the “Courses (p. 1)” tab.

Courses

Computer Science (CSC) (p. 1), Cybersecurity (CYB) (p. 2), Data Analytics (DAT) (p. 2), Mathematics (MAT) (p. 2)

Computer Science (CSC)

CSC 501 Introduction to Programming for Data Analytics 3 Credits
This foundational course will teach you the basics of computer programming using the Python language. You will design, code, test, and debug computer programs for textual and graphical applications.
Offered: every fall, spring, & summer.

CSC 501L Introduction to Programming for Data Analytics Lab 0 Credits
Required lab for CSC 501.
Corequisite: CSC 501.
Offered: Summer.

CSC 502 Data Structures and Algorithms 3 Credits
The primary focus of this course is data structures and their accompanying algorithms, including recursive algorithms. In order to judge between competing algorithms or alternative data structures, we will use analysis to discover the time and memory bounds of various approaches. We will also use object oriented programming as a useful way of constructing abstract data types and in general structuring complex programs. Several debugging tools and approaches will be explored, especially hand tracing of algorithms. The Python programming language will be our main vehicle.
Prerequisite: CSC 501 or CSC 111 as prerequisite. Corequisite: CSC 502L.
Offered: every fall, spring, & summer.

CSC 502L Structures and Algorithms for Data Analytics Lab 0 Credits
Required lab for CSC 502.
Corequisite: CSC 502.
Offered: Summer.
- CSC 530 Operating System Design and Distributed Computing 3 Credits
  The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster.
  Prerequisites: Minimum grade of C in CSC 502 & CSC 502L.
  Offered: every fall.
- CSC 530L Operating System Design and Distributed Computing Lab 0 Credits
  Required lab for CSC 530.
  Prerequisites: Minimum grade of C in CSC 502 & CSC 502L.
  Offered: every fall.

Cybersecurity (CYB)

CYB 500 Cybersecurity Principles 3 Credits
This course examines the landscape and the broad areas of cybersecurity which includes topics such as: Symmetric & Public-Key Encryption, Access Control, Database Security, Malware, DoS (Denial-of-Service) Attacks, Intrusion Detection & Firewalls, Software Security, Security Management & Policies, Internet Security, and Legal & Ethical Aspects of Cybercrime. Students will also complete hands-on labs and exercises to reinforce their working knowledge of computer, network and information security topics.
  Prerequisites: Minimum grade of C- in DAT 513 & DAT 513L; may be taken concurrently.
  Offered: every fall & spring.
- CYB 500L Cybersecurity Principles Lab 0 Credits
  Required lab for CYB 500.
  Prerequisites: Minimum grade of C- in DAT 513 & DAT 513L; may be taken concurrently.
  Offered: every fall & spring.
- CYB 510 Cybersecurity Policies, Ethics, and Law 3 Credits
  This course focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series.
  Prerequisites: A minimum grade of C- in CYB 500.
  Offered: every spring.
- CYB 520 Ethical Hacking and Penetration Testing 3 Credits
  This course provides an in-depth understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Students will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking.
  Prerequisites: Minimum grade of C- in CYB 500 and CYB 500L.
  Offered: every spring.
- CYB 520L Ethical Hacking and Penetration Testing Lab 0 Credits
  Required lab for CYB 520.
  Prerequisites: Minimum grade of C- in CYB 500 and CYB 500L.
  Offered: every spring.
- CYB 540 Network and Internet Security 3 Credits
  The purpose of this course is to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (e.g., SSL, S/MIME, IP Security, IEEE 802.11). This course will also cover security as well as code reviews and software penetration testing. Finally, we will cover the first part of the course will cover a concise survey of the cryptographic algorithms and protocols underlying network security applications, including Extensible Authentication Protocol, S/MIME, IP Security, SSL/TLS, IEEE 802.11.
  Prerequisites: Minimum grade of C- in CYB 500, CSC 502, and DAT 513.
  Offered: every fall.
- CYB 540L Network and Internet Security Lab 0 Credits
  Required lab for CYB 540.
  Prerequisites: Minimum grade of C- in CYB 500, CSC 502, and DAT 513.
  Offered: every spring.

Learning Goals & Objectives
Learning Objectives. Upon completing the MS program, students will be able to:
  - Perform information security risk assessment, identify potential threats, and develop threat mitigation strategies.
  - Describe individual privacy rights, related laws and regulations, and the use of information assurance technologies to support the enforcement of these rights.
  - Describe the responsibilities of all levels of users related to the threats against information systems.
  - Describe security design principles and identify security mechanisms to implement desired security principles.
  - Implement security defense technologies.
  - Identify malicious activities and attacks, and recommend appropriate response capabilities.
  - Carry out incident response activities and support cyber-crime investigation.
  - Perform audit procedures, evaluate the strengths and weaknesses of the security mechanisms, and develop contingency plans.
• Communicate information security concepts to individuals with diverse levels of computing skills.