Overview
The Cybersecurity Master’s program curriculum consists of 10 courses (30 credits) that can be completed over 12 months, following a hybrid (on-campus and online) delivery model. Students who track with their entry cohort can complete the program in three semesters (fall, spring, summer). Students may select to complete a thesis through two courses instead of a capstone project and fifth elective. Classes will be offered in the evenings and during the weekends.

Prerequisites
All undergraduate majors are welcomed. Professional knowledge or experience equivalent to the following four courses is required:

1. Computer Programming with basic algorithms (in C, C++, Java, R or Python) (e.g., CISC 5004 Computer Programming C++ or CISC 5380 Programming with Python)
2. Applied Statistics and Probability or Discrete Mathematics (e.g., CISC 5420 Applied Statistics and Probability or CISC 5002 Discrete Structures).

Bridging courses are available for students who are missing one or more of the aforementioned prerequisites. With the permission of the Program Director, these courses can be taken concurrently with the cybersecurity courses. If you are required to take these courses, it will be stated in your admissions letter and the courses must be taken during the first semester.

CIP Code
You can use the CIP code to learn more about career paths associated with this field of study and, for international students, possible post-graduation visa extensions. Learn more about CIP codes and other information resources.

Requirements

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISC 5009</td>
<td>Network Essentials ¹</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5650</td>
<td>Cybersecurity Essentials ¹</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5750</td>
<td>Information Security and Ethics</td>
<td>3</td>
</tr>
<tr>
<td>Five elective courses, with the option to pursue an internship</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>One selection from the following: ²</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>Master’s Thesis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CISC 6095 &amp; CISC 6096</td>
<td>Master’s Thesis in MSCY I and Master’s Thesis in Cybersecurity II</td>
<td></td>
</tr>
<tr>
<td>Capstone and Elective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CISC 6090</td>
<td>Capstone Project in Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>One additional elective from the selection below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Credits 30

¹ CISC 5009 Network Essentials and CISC 5650 Cybersecurity Essentials must be taken in the first semester.

² Capstone and thesis courses can only be taken during the second or third semester.

Electives
Courses in this group have the CYSM attribute.

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISC 5550</td>
<td>Cloud Computing</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5660</td>
<td>Data Science for Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5710</td>
<td>Introduction to Behavioral and Physical Biometrics</td>
<td></td>
</tr>
<tr>
<td>CISC 5728</td>
<td>Security of e-Systems and Networks</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5770</td>
<td>Intelligence in Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CISC 5850</td>
<td>The Social Network</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6070</td>
<td>Red Teaming</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6091</td>
<td>Cybersecurity Practicum</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6600</td>
<td>Cloud Computing Security</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6630</td>
<td>Wireless Security</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6640</td>
<td>Privacy and Security in Big Data</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6650</td>
<td>Forensic Computing</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6660</td>
<td>Applied Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6670</td>
<td>Artificial Intelligence for Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6680</td>
<td>Intrusion Detection and Network Forensics</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6690</td>
<td>Cybersecurity in Business</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6750</td>
<td>IOT Forensics and Security</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6800</td>
<td>Malware Analytics and Software Security</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6850</td>
<td>Leadership and Management in Cybersecurity</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6860</td>
<td>Cybersecurity: Technology, Policy, and Law</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6880</td>
<td>Blockchain Technology</td>
<td>3</td>
</tr>
<tr>
<td>CISC 6920</td>
<td>Incident Response and Risk Management</td>
<td>3</td>
</tr>
<tr>
<td>CISC 7050</td>
<td>Penetration Testing</td>
<td>3</td>
</tr>
<tr>
<td>CISC 8150</td>
<td>Special Topics in Cybersecurity</td>
<td>3</td>
</tr>
</tbody>
</table>