The Master of Science in Cybersecurity degree program requires 32 credit hours of coursework (including a 5 credit practicum project course). Two of the core courses, which students in each specialization will take, will provide a broad overview of technology and policy dimensions of cybersecurity. Students are required to take a third core course that comes from one of the other specializations; e.g., a policy specialization student must take a course from the cyber-physical or information security track. Finally, a practicum project (5 credit hours) with common learning objectives across all participating units will be a core requirement. Each participating unit will decide required and elective courses for the MS Cybersecurity degree specialization offered by it (a total of 18 credit hours). These requirements have been defined by the participating units and are described in the next section.

Although all three participating schools will offer a single degree, MS Cybersecurity, the focus of the degree will depend on the specialization defined by the offering unit. In particular, each unit will offer the following specializations for the MS degree in Cybersecurity.

- The School of Computer Science (CS) offers the MS Cybersecurity degree with an information security specialization.
- The School of Electrical and Computer Engineering (ECE) offers the MS Cybersecurity degree with cyber-physical systems specialization.
- The School of Public Policy (PUBP) offers the MS cybersecurity degree with a policy specialization.

### Program of Study

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credit Hours</th>
</tr>
</thead>
</table>

#### Required Core Courses:
- CS 6035 Introduction to Information Security 3
- PUBP/CS/MGT 6725 Information Security Policies and Strategies 3
- CS/ECE/PUBP 6727 Cyber Security Practicum 5
- Elective course CS/PUBP/ECE 6000-level 3

Specialization Requirements (see below for specialization specific requirements) 18

Total Credit Hours 32

1 Public Policy students must take CS or ECE elective

#### GPA/Grade Requirements:
- Students must achieve a grade-point average of at least 3.0 to graduate
- No course grades below ‘C’ will count toward graduation
- Students must take all master’s degree coursework on a letter-grade basis

### Information Security Specialization:
- CS 6260 Applied Cryptography 3

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credit Hours</th>
</tr>
</thead>
</table>

### Cyber-Physical Systems Specialization:
- ECE 6320 Power Systems Control and Operation 3
- ECE 8813 Special Topics (Introduction to Cyber-Physical Electric Energy Systems) 3
- ECE 8813 Special Topics (Introduction to Cyber-Physical Systems Security) 3
- ECE 8803 Special Topics (Computational Aspects of Cyber-Physical Systems or Cyber Physical Design and Analysis) 3

Select two courses: 6

- ECE 6550 Linear Systems and Controls
- ECE 6607 Computer Communication Networks
- ECE 6615 Sensor Networks
- ECE 6102 Dependable Distributed Systems
- ECE 6323 Power System Protection
- ECE 8813 Special Topics (Advanced Computer Security)
- ECE 8813 Special Topics (Network Forensics)
- ECE 8813 Special Topics (Smart Grids)
- ECE 8803 Special Topics (Advanced Topics in Malware)
- ECE 8873 Special Topics (Advanced Hardware Oriented Security and Trust)

Total Credit Hours 18
The Master of Science in Cybersecurity is also offered online.

For more information, visit: Online Master of Science in Cybersecurity.