

MASTER OF SCIENCE IN CYBERSECURITY

Graduate study in Cybersecurity is open to students who have completed undergraduate coursework in Computer Science, Cybersecurity, Digital Forensics, Information Systems, or a closely related technical field. Applicants with bachelor's degrees in other fields may also be considered if they have equivalent academic preparation, technical coursework, or relevant professional experience. Applicants who do not have sufficient technical preparation may be required to complete stem work courses to ensure a minimum level of technical competence. Stem work decisions are made on an individual basis by the department chair.

Additional information: Reference the Program Landing Page (<https://www.shsu.edu/programs/graduate/information-assurance-and-cybersecurity/>) for additional information, such as cost, delivery format, contact information, or to schedule a visit.

Applicants seeking admission to the graduate program in Cybersecurity must submit the following directly to the Office of Graduate Admissions (<https://www.shsu.edu/dept/graduate-admissions/prospective-students.html>):

1. Graduate Application (<http://www.shsu.edu/admissions/apply-texas.html>)
2. Application Fee (<http://www.shsu.edu/dept/graduate-studies/application-fee.html>)
3. Official transcript from the baccalaureate degree granting institution
4. Up-to-date resume
5. Two letters of recommendation that address the applicant's qualification for graduate study
6. Auto-admission eligibility is limited to SHSU Computer Science (CS) students who are in their final semester of study toward, or who have already graduated with, a BS degree from the Department of Computer Science and who have a minimum overall undergraduate GPA of 3.0.

SHSU CS students applying for our MS program during their final undergraduate semester may be considered for auto-admission. However, final admission is contingent upon successful completion of their BS degree and maintenance of a minimum overall undergraduate GPA of 3.0 at the time of graduation.

SHSU CS students who wish to enroll in graduate-level MS courses offered by the Department of Computer Science during their final undergraduate semester must apply for dual enrollment. Approval for dual enrollment does not guarantee regular admission to an MS program in the Department of Computer Science. At the end of the final semester, the student's admission status will be reviewed to confirm successful completion of the BS degree and continued satisfaction of the minimum overall undergraduate GPA requirement of 3.0. If these requirements are not met, the student may be denied regular admission, placed on probationary admission status, or subject to further review.

This degree is accessible to students who have completed undergraduate Computer Science or Criminal Justice majors or minors and to those with baccalaureate degrees in technical fields with the equivalent of a Computer Science or Criminal Justice minor in formal coursework or professional experience. Applicants who do not possess the appropriate academic, technical, or experiential backgrounds may be required to take stem work courses. In addition, admission preference is given to applicants with a GPA of 3.0 or greater.

Stem Requirement

At the minimum, students are expected to present a background comparable to that provided in the following courses as described in the Undergraduate Catalog of Sam Houston State University:

Prerequisite Courses

Code	Title	Hours
Required Courses		
COSC 2327	Introduction to Computer Networks	3
COSC 3318	Data Base Management Systems	3
MATH 1420	Calculus I	4
STAT 3379	Statistical Methods in Practice	3

Students **who have not fulfilled** the prerequisites in formal coursework **are required** to take one or more of the undergraduate/graduate stem courses, in addition to the 30 semester credit hours required in the MS in Cybersecurity.

Stem Course Requirement

Code	Title	Hours
Stem Course Requirement		
COSC 5301	Quantitative Foundations of Computer Science	3
COSC 5302	Computer Science Core Topics	3
DFSC 4399	Foundations of Cyber Security and Digital Forensics	3

The degree requires a minimum of thirty hours of graduate credit. All MS students in the Non-Thesis Option are obligated to fulfill and achieve a passing grade in written or oral comprehensive exams for core subjects where they obtained a grade of B or lower. Exams are conducted during their terminal semester. Should a student fail one or more examinations, a re-examination shall be permitted per department approval. A third examination may be permitted only with the approval of the appropriate academic dean and the department. Students must be enrolled at SHSU in the semester in which the comprehensive exams are administered.

An MS Project or Thesis committee will be established either before or during the student's penultimate semester. The committee should consist of a committee chair (supervisor) and a minimum of two additional committee members, all holding the appropriate graduate faculty status. With the approval of the department, academic dean, and Dean of The Graduate School, the committee may include one member who is not employed by SHSU, as per Academic Policy Statement 950601. The selection of the committee chair hinges on the student's preference, faculty availability, and expertise. Once a faculty member agrees to assume the role of chair, the student, under the chair's guidance, will proceed to select the remaining committee members. Subsequently, the committee's constitution needs approval from both the Graduate Coordinator and the Dean. Any alterations to the committee's composition will similarly require approval through the same process.

Plan 1 - Master of Science in Cybersecurity (Thesis Option)

The Master of Science in Cybersecurity (Thesis Option) can better prepare students interested in pursuing Ph.D. degrees or related fields, providing valuable research experience and a strong academic foundation. It also provides students with greater flexibility and choice in how they tailor their academic experience to align with their interests and goals.

Code	Title	Hours
Master of Science in Cybersecurity (Thesis Option)		
Specified Courses		
COSC 5325	Operating System Security	3
COSC 5335	Database Security	3
COSC 6049	Thesis ¹	3
COSC 6348	Thesis ¹	3
DFSC 5310	Principle and Policy in Information Assurance	3
DFSC 5315	Network and Cyber Security	3
DFSC 5336	Business Continuity Management	3
Required Track Courses ²		9
Total Hours		30

¹ Once enrolled in a thesis course, the student must enroll in a thesis course until graduation.

² See MS in Cybersecurity Tracks course listings below.

Plan 2 - Master of Science in Cybersecurity (Non-Thesis Option)

The Master of Science in Cybersecurity (Non-Thesis Option) requires coursework and completion of a master's project. This plan is designed for students who want to gain practical experience by applying cybersecurity knowledge and skills to a focused project while also completing a structured graduate program.

Code	Title	Hours
Master of Science in Cybersecurity (Non-Thesis Option)		
Specified Courses		
COSC 5325	Operating System Security	3
COSC 5335	Database Security	3
DFSC 5310	Principle and Policy in Information Assurance	3
DFSC 5315	Network and Cyber Security	3
DFSC 5336	Business Continuity Management	3
DFSC 6347	Directed Management and Development Project ¹	3
Prescribed Electives		
Select one graduate course in DFSC or COSC ²		3
Required Track Courses ³		9
Total Hours		30

¹ Once enrolled in DFSC 6347, the student must enroll in this course until graduation.

² COSC 5301 and COSC 5302 do not count towards the degree plan.

³ See MS in Cybersecurity Tracks course listings below.

Plan 3 - Master of Science in Cybersecurity (Professional Option)

The Master of Science in Cybersecurity (Professional Option) requires only coursework without a thesis or MS project. This plan is suggested for working professionals and individuals seeking to enhance their skills and knowledge in cybersecurity.

Code	Title	Hours
Master of Science in Cybersecurity (Professional Option)		
Specified Courses		
COSC 5325	Operating System Security	3
COSC 5330	Malware	3
COSC 5335	Database Security	3
DFSC 5310	Principle and Policy in Information Assurance	3
DFSC 5315	Network and Cyber Security	3
DFSC 5336	Business Continuity Management	3
DFSC 5338	Ethical Hacking	3
Required Track Courses ¹		9
Total Hours		30

¹ See MS in Cybersecurity Tracks course listings below.

MS in Cybersecurity Tracks

Code	Title	Hours
Cybersecurity Track		
Select three graduate courses in DFSC or COSC ¹		9

¹ COSC 5301 and COSC 5302 do not count towards the degree plan.

Code	Title	Hours
Artificial Intelligence Track		
COSC 5313	Artificial Intelligence	3
COSC 6315	Machine Learning	3
DFSC 5340	Special Topics in Digital Forensics	3

The Texas Higher Education Coordinating Board (THECB) marketable skills initiative is part of the state's **60x30TX plan** and was designed to help students articulate their skills to employers. Marketable skills are those skills valued by employers and/or graduate programs that can be applied in a variety of work or education settings and may include interpersonal, cognitive, and applied skill areas.

The MS in Cybersecurity is designed to provide graduates with the following marketable skills:

- Establish and operate an investigator's lab, and process digital evidence.
- Develop plans to safeguard digital files against unauthorized modification and destruction.
- Create plans and implement strategies for preventing attacks to a network.
- Analyze and assess risk and identify vulnerabilities in an organization's network.
- Acquire the professional competency and cybersecurity expertise necessary for roles and responsibilities in business, industry, and governmental positions.