MASTER OF SCIENCE IN INFORMATION ASSURANCE AND CYBERSECURITY

Graduate study in Information Assurance and Cybersecurity is accessible both to students who have completed undergraduate Computer Science or Management Information Science majors or minors and to those with baccalaureate degrees in technical fields with the equivalent of a Computer Science or Management Information Science 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 to ensure a minimum standard of technical competence. Stem work decisions are made on an individual basis by the department chair.

Applicants seeking admission to the graduate program in Information Assurance and 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. Official GRE scores
6. Two letters of recommendation that address the applicant's qualification for graduate study

Admission preference is given to applicants with a GPA of 3.0 or higher.

GRE Waiver Requests:

In order obtain a waiver of the GRE score requirements, applicants must have either

1. an awarded M.S. degree from an accredited institution of higher education, or
2. 5+ years of full-time relevant work experience beyond the baccalaureate degree.

The Master of Science in Information Assurance and Cybersecurity program has a total of 30 semester credit hours. Students will be required to complete a written comprehensive examination in core subjects where they received a grade of B or lower, before graduation. Students also may be required to supplement their written responses in an oral examination. Students must be enrolled the semester in which they take comprehensive examinations.

The department chair assigns a committee to each student at the time the student registers for DFSC 6347. The advisory committee consists of graduate faculty from the Department of Computer Science. Once enrolled in DFSC 6347, a student must be continually enrolled in each major semester until graduation.

Code	Title	Hours
Master of Science in Information Assurance and Cybersecurity		
Specified Courses		
COSC 5325	Operating System Security	3
COSC 5335	Database Security	3
DFSC 5310	Princple& Policy-Info Assuranc	3
DFSC 5315	Network and Cyber Security	3
DFSC 5336	Business Continuity Management	3
DFSC 6347	Directed Mgt & Development Prj [1]	3
Electives		
Select four graduate courses in DFSC or any approved COSC graduate courses [2]		12
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.

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 Information Assurance and 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/asses risk and identify vulnerabilities in an organizations network
- Acquire the professional competency and cybersecurity expertise necessary for roles and responsibilities in business, industry, and governmental positions.