## GRADUATE INTERNSHIP IN CYBER SECURITY

## GENERAL GUIDELINES

An internship is a critical part of your college experience at SFA, and the real-world experience you can gain will provide you with a competitive edge when beginning your career. Online job boards and internet search are convenient ways to search for career opportunities. Unfortunately, scammers utilize internet search results, online job boards, and advertisements to target unsuspecting college students looking for job openings and internships. To help reduce your risk and educate yourself on the signs of an internship scam, please be sure to review the posted information at the Department of Computer Science Internship website.

**Course Description**: One to three semester hours. Supervised on-the-job training in one or more facets of the field of cyber security.

**Prerequisites:** Graduate student in good standing in the Department of Computer Science, overall grade point average of 3.0 or higher, completion of 12 hours of graduate work in computer science, and consent of the graduate coordinator or CSCI 5185 course supervisor.

May be repeated for three hours credit. No more than 3 hours of internship may count toward a graduate degree in Cyber Security in the Department of Computer Science. May be used to replace the capstone requirement of the graduate degree in Cyber Security. **Pass or Fail**.

Receiving a failing internship grade or withdrawing from the course due to an unsatisfactory evaluation or termination by the employer shall disqualify the student from further enrollment in any internship course.

### General Information

The working hours / credit hours relationship depends upon the type of position and the number of hours worked per week. Ordinarily, a three-credit hour internship course should include at least 180 working hours. Deviations in the working hour-credit relationship must be approved in advance by the internship director.

Students can apply for graduate credit for an internship provided they meet the general requirements stated above and is detailed in the following section.

### Student Responsibilities & General Workflow

1. Obtain employment in a position involving direct work relevant to cyber security.
2. Complete the Internship Application and Approval form. This form provides contact information of your internship supervisor, documents the internship duties, and aids in validation of meeting the prerequisites for credit. The form must be received and approved prior to commencing the internship to receive course credit. Please note the following:
    a. Applications received within ten business days of the internship start date may not receive full consideration.
    b. Applications received and requesting credit within a term commencing in less than ten business days will be rejected.

    c. Internships with organizations outside of the East Texas area involving only remote work will not be considered. An exception may be granted for organizations that are publicly traded.
    d. Internships with majority work related to cyber security education will not be considered.
3. After receiving a permit from the internship director, enroll in the corresponding CSCI 5185 section for the indicated term.
4. Perform duties of position as required by company.
5. Attend one or two internship group meetings during the semester as announced by the internship director (you will be contacted about the meeting). This requirement may be waived for those employed outside the Nacogdoches area.
6. Participation in at least one outreach event discussing your internship experience. This may include presenting at a computer club meeting, serving on a panel, etc. This will be scheduled in coordination with the internship director.
7. Your work supervisor will be sent a performance appraisal to complete prior to the completion of your internship.
8. Provide a public presentation describing the employer's application process, the duties performed, learning experiences, and effects of the internship on your education and future. This presentation is to department faculty and students involved in the cyber security program.