



**Academic Plan**  
**Cybersecurity Certificate**  
EFFECTIVE CATALOG YEAR 2018-2019



## Required Courses

**CSC 145- Information Security Fundamentals – 3 credits**

Introductory course in which students explore the principles of information assurance, with emphasis on current threats and vulnerabilities to develop an information security plan to mitigate risk. Information security and assurance issues are explored and a multidisciplinary approach is discussed that examines security policies, models, and mechanisms for confidentiality, integrity, and availability. Theory/Lab

**CSC 150- Computer Science I – 3 credits**

An introduction to computer programming. Focus on problem solving, algorithm development, design, and programming concepts. Topics include sequence, selection, repetition, functions, and arrays.

**CSC 234- Software Security – 3 credits**

This course will make use of hands-on exercises in compiled and web-based software to illustrate attack methodologies and techniques that lead to software vulnerabilities that violate fundamental security principles. Attacks and mitigation strategies related to filter evasion, session management, input validation, buffer overflows, and related areas will be emphasized. Prerequisite: CSC 150

**CSC 250- Computer Science II – 3 credits**

Problem solving, algorithm design, standards of program style, debugging and testing. Extension of the control structures and data structures of the high-level language introduced in CSC 150. Elementary data structures and basic algorithms that include sorting and searching. Topics include more advanced treatment of functions, data types such as arrays and structures, and files. Prerequisite: CSC 150