Cybersecurity and Healthcare IT

Degree Type
Associate of Science

The Cybersecurity and Healthcare IT degree meets the need for healthcare providers and associated businesses to be confident that every aspect of their operation is electronically secure. As the functions of healthcare include scheduling, storage of images, filling prescriptions, billing, and more are handled and stored using information technology, the need to build electronic and data transfer systems to support these functions, and to protect the information, has dramatically increased. With this shift, the vulnerability of healthcare records has also increased through errors, acts of negligence and malice. The workforce responsible for this electronic information must be skilled in assuring confidentiality, integrity and availability of IT systems and networks. This unique program focuses on the integration of the technology along with the needs of the healthcare industry increasing the value of the cybersecurity professional.

Cybersecurity is the practice of protecting computer systems against unauthorized access or attack and maintaining the smooth functioning of information systems at all levels. At present, programs that provide such Cybersecurity training are not widely available, and the additional concentration on healthcare is a unique aspect of this program.

Applicants to the Cybersecurity and Healthcare IT Program must meet the general admission requirements to the College and interview with the Program Director. It is expected that applicants already have a basic knowledge of computer hardware and software. Applicants who do not possess this knowledge may be required to take additional courses to meet this need. Attending college part-time will take more than two years to complete.

Students must earn a grade of “C” or higher in all CYBS/CSCI technology courses required for graduation to progress within the program and graduate.

Students will be required to become a member of Infragard as a prerequisite for the Digital Forensics course. Students with known criminal background or legal actions may not be able to become a member of Infragard and may be denied enrollment and/or progression in the program. These students are advised to seek an alternate education program. Students will be required to sign a program code of conduct that has a zero tolerance policy. Violation of the code of conduct will be grounds for removal from the program. Students who are unable to pass a criminal background check may find it difficult to obtain or stay employed in the Cybersecurity industry.

Program Mission

To develop and train cybersecurity technology professionals who can help companies manage and protect their systems and utilize their skills in technology as well as within a medical environment.

Program / Student Outcomes

The proposed program will provide students with a strong foundation of understanding in cybersecurity. Students will learn:

- the broad discipline of cybersecurity and develop a foundation of knowledge of the field
- to write clearly and effectively for defined audiences through a variety of strategies
- the purpose behind their field of study, how to best interact with the people in their work environment and the career path that is best aligned with their personal goals
- how to use multiple operating systems commonly found in the Cybersecurity Technology field today
- basic security principles for information assurance
- the basics of descriptive and inferential statistics
- the basics of the web development process and types of attacks that can occur
- computer networking through the introduction of the Open Systems Interconnection (OSI) model, the TCP/IP protocol suite, routing and switching protocols, Wide Area Network services, and network design & implementation

- a programming language and be able to design and implement simple programs dealing with numerical and string processing
- to implement, maintain and protect a Microsoft Windows Server Domain
- to perform ordinary tasks in the Linux operating systems
- the methods in which emerging technologies can be deployed on current and future platforms
- how to succeed in an information technology position through an Internship or Capstone course

NOTE

* Many courses have co/prerequisites. See course descriptions for requirements.

	Total Credits	**62-66**

Course Sequencing

First Year: Fall Semester

Item #	Title	Credits
CSCI101R	Computer Architecture and Operating Systems	3
CYBS101R	Principles of Information Assurance	3
CSCI110R	Introduction to Networks	3
CSCI186R	Introduction to Operating Systems	3
MATH110R	Functions & Modeling I	4

First Year: Spring Semester

Item #	Title	Credits
CYBS120R	Network Security	3
CYBS130R	Enterprise Security Management	3
CYBS140R	Secure Electronic Commerce	3
CSCI175R	Introduction to C++	4
ENGL102R	College Composition	3-4

Second Year: Fall Semester

Item #	Title	Credits
CYBS110R	Topics in Healthcare Information Technology	3
CSCI203R	Introduction to Linux	3
CYBS250R	Digital Forensics	3
MATH106R	Statistics I	4
	English/Humanities/Fine Arts/World Language/Science/ Mathematics or Social Science Elective	3-4

Second Year: Spring Semester

Item #	Title	Credits
CYBS200R	Electronic Medical Records Systems & Information Assurance Certification and Accreditation Process (EMRS/IACAP)	3
CSCI296R	Technology Capstone	3
	Social Science Elective	3
	Science Elective	3-4
	Humanities/Fine Arts/World Language Elective	3