Information Systems Security (SEC)

SEC 110. Security Concepts. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-2.0. Work-0.0
This course introduces the concepts and issues related to securing information systems and the development of policies to implement information security controls. Topics include the historical view of networking and security, security issues, trends, security resources, and the role of policy, people, and processes in information security. Upon completion, students should be able to identify information security risks, create an information security policy, and identify processes to implement and enforce policy.

SEC 150. Secure Communications. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-2.0. Work-0.0
This course provides an overview of current technologies used to provide secure transport of information across networks. Topics include data integrity through encryption, Virtual Private Networks, SSL, SSH, and IPSec. Upon completion, students should be able to implement secure data transmission technologies.

SEC 151. Introduction to Protocol Analysis. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-3.0. Work-0.0
This course introduces protocol analysis. Topics include protocol analysis tools, TCP/IP concepts, Internet protocols, network traffic analysis, monitoring network traffic, network security protocol analysis, and understanding data flow through protocol analysis. Upon completion, students should be able to perform simple protocol analysis to determine baseline network performance and identify anomalies.
Prerequisites: Take CTI 120 SEC 110 AND NOS 120; MINIMUM GRADE C.

SEC 160. Security Administration I. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-2.0. Work-0.0
This course provides an overview of security administration and fundamentals of designing security architectures. Topics include networking technologies, TCP/IP concepts, protocols, network traffic analysis, monitoring, and security best practices. Upon completion, students should be able to identify normal network traffic using network analysis tools and design basic security defenses.

SEC 251. Advanced Protocol Analysis. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-3.0. Work-0.0
This course is designed to provide advanced understanding of protocol analysis. Topics include advanced network protocol security analysis, data parsing, monitoring scanning logs, and network intrusion identification. Upon completion, students should be able to apply best practices in protocol analysis and apply the results to IT security frameworks.
Prerequisites: TAKE SEC 151 NET 125 AND CSC 121; MINIMUM GRADE C

SEC 258. Security Compliance. 3.0 Credits. Class-2.0. Clinical-0.0. Lab-3.0. Work-0.0
This course introduces information security compliance and standards along with how they apply to corporate IT environments. Topics include ISO standards, government NIST frameworks, federal and state compliance requirements, security policies, incident response and business continuity planning. Upon completion, students should be able to apply compliance and availability requirements to corporate data enterprise scenarios.
Prerequisites: Take SEC 110, minimum grade of C

SEC 285. Systems Security Project. 3.0 Credits. Class-1.0. Clinical-0.0. Lab-4.0. Work-0.0
This course provides the student the opportunity to apply the skills and competencies acquired in the program that focus on systems security. Emphasis is placed on security policy, process planning, procedure definition, business continuity, compliance, auditing, testing procedures and systems security architecture. Upon completion, students should be able to design and implement comprehensive information security architecture from the planning and design phase through implementation.
Prerequisites: Take all: CTI 110, CTI 120, and CTS 115