CITY - CYBERSECURITY - CERTIFICATE OF ACHIEVEMENT

PROPOSAL INFORMATION

Action Proposed: New Program

Proposal Originator: David Kennemer

Origination Date:04/05/2017

Proposed Start: Fall 2018

Need for Proposal:
This Certificate of Achievement is being created in response to labor market demands in the cybersecurity field.

Attached Documents:
[Advisory Recommendation](#)
[Advisory Approval](#)
[LMI](#)

PROGRAM & AWARD INFORMATION

Award Description:
The Cybersecurity Certificate of Achievement prepares students to work in the Information Security and Assurance (ISA) industry. Emphasis is placed on methods for protecting information systems and data from cyber incidents through policy analysis, information systems security, ethical hacking, and digital forensics. The Cybersecurity curriculum follows the National Training Standard for Information Systems Security designation sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS).

Award Notes:
The goal of this award is to provide students with the skills and experience necessary to obtain employment in the ISA industry. Outcomes include the skills necessary to:
1. Identify and discuss the foundational technical concepts, industry standards, and state and federal legislation concerning the security of information and technology assets and the effects it has on managerial roles and organizational policies.
2. Define and identify risk, perform vulnerability assessments, and conduct penetration testing on various network technologies following applicable ethics and code of conduct.
3. Design, implement, and maintain a complete enterprise security strategy for various endpoints, cloud technology, and wired and wireless networks.
4. Discuss, develop, and implement a security awareness training program as it pertains to various levels of information and technology assets.
5. Communicate and understand the history of computer forensics and cybercrime in order to establish procedures for identifying, acquiring, and handling digital evidence in the event of a computer or network related incident or crime.

Program Description:
n/a

Program Goals:
n/a

Program Emphasis:

Career Options:
Careers in the cybersecurity or information assurance field include: information security consultant, security administrator, security analyst, security engineer, security auditor, incident responder, penetration tester, vulnerability assessor, support technician, systems administrator, network administrator, and network specialist. Note: Some careers in the cybersecurity field require education beyond the associate degree in either Cybersecurity or Information Assurance.

COURSES REQUIRED FOR THE MAJOR: UNITS

INWT 101	Introduction to Information Security *Active*	3
INWT 111	Windows Desktop Professional *Active*	3
INWT 112	Windows Server Professional *Active*	3
INWT 120	Network+ Certification Training *Active*	4
INWT 140	Security+ Certification Training *Active*	3
INWT 145	Linux+ Certification Training *Active*	4
INWT 170	Cybersecurity Analyst+ (CySA+) Certification Training *Active*	3
INWT 200	Certified Ethical Hacking (CEH) Certification Training *Active*	4
INWT 205	CompTIA Advanced Security Practitioner (CASP) Certification Training *Active*	4
INWT 210	Introduction to Computer Forensics Investigation *Active*	3

SELECT ONE COURSE FROM THE FOLLOWING: UNITS

INWT 100	A+ Certification Training *Active*	4
INWT 105	Project+ Certification Training *Active*	4
INWT 135	Certified Secure Computer User (CSCU) *Active*	3
BUSE 092	Introduction to Business Communication *Active*	3

Total Units   37 - 38

DATES & CODES
CIC Approval: 12/14/2017
Board Approval: 01/25/2018   **TOP Code:** 0708.00
State Approval: 06/11/2018   **State Approval (Unique) Code:** 36754

Subject Area: Information, Network, and Web Technologies   Report Run: 10/29/2020 12:23 PM

Program Area: Computer Information Systems   Program ID: 3424