OUR GOAL IS YOUR SUCCESS.

ACCELERATED PROFESSIONAL PROGRAM

SATURDAYS AT THE NORTH CAMPUS
CYBERSECURITY CERTIFICATE PROGRAM (786)

- This is a great opportunity to expand and upgrade your credentials and enhance employment opportunities.
- There are 8 courses in this program.
- Each course is 8 weeks.
- It is suggested that the courses be taken in sequence. CIT 285 must be taken in the final semester.

This certificate program is designed to prepare students for entry-level careers related to Cybersecurity. The program objectives are based on the guidelines in the Cybersecurity Workforce Framework published by the National Initiative for Cybersecurity Careers and Studies (NICCS).

CERTIFICATE REQUIREMENTS			
SPRING 2019:			
CIT-115-NC35H	Introduction to Information Technology	3 credits	1/19/19 - 3/9/19
CIT-175-NC35H	Cyberspace Vulnerabilities and Risks	3 credits	3/16/19 – 5/11/19
SUMMER 2019:			
CIT-180-NC35H	Computer Forensics 1	3 credits	5/18/19 – 7/6/19
CIT-181-NC35H	Principles of Information Security	4 credits	7/13/19 – 8/31/19
FALL 2019:			
CIT-185-NC35H	Network Security	3 credits	9/7/19 – 10/26/19
CIT-186-NC35H	Intrusion Detection and Prevention	3 credits	11/2/19 – 12/14/19
SPRING 2020:			
CIT-282-NC35H	Advanced Cybersecurity Topics	3 credits	1/18/20 – 3/7/20
CIT-285-NC35H	Cybersecurity Capstone	3 credits	3/14/20 – 5/9/20
FOR MORE INFORMATION, CALL OR VISIT THE CCAC NORTH CAMPUS ADVISING OFFICE, 412-369-3740, ROOM 1004A			

Revised: 11/21/2018

OUR GOAL IS YOUR SUCCESS.

CIT – CYBERSECURITY
CERTIFICATE PROGRAM (786)

This certificate program is designed to prepare students for entry-level careers related to Cybersecurity. The program objectives are based on the guidelines in the Cybersecurity Workforce Framework published by the National Initiative for Cybersecurity Careers and Studies. (NICCS).

Upon successful completion of the program, the graduate will:

1. Identify, describe and analyze vulnerabilities, threats and risks for critical information assets.
2. Plan, implement and maintain security measures and controls to protect critical information assets.
3. Prevent, detect, analyze and respond to system intrusions and data breaches.
4. Analyze and evaluate emerging cybersecurity risks and solutions with creative and critical thinking and research skills.

Course Descriptions:

CIT 115 Introduction to Information Technology 3 credits

This course explores technical issues involved with computers and information technology. Topics include computer hardware and components, operating systems, file storage, networking fundamentals, digital media, database systems and the Internet structure & organization. Students research various information technology issues using the Internet and in-class or simulated lab exercises in a personal computer environment.

CIT 175 Cyberspace Vulnerabilities and Risks 3 credits

This course introduces students to the fundamentals of Cybersecurity, such as cybersecurity goals, vulnerabilities, threats, and risks. Students also learn to use the methods and tools for cybersecurity vulnerability scanning and risk assessment.

CIT 180 Computer Forensics 1 3 credits

(Prerequisite: CIT-115 or instructor approval)

This course introduces students to the fundamentals of the computer forensics field and technology. Students will obtain essential knowledge of the computer forensics profession, legal issues and procedures of computer investigations and digital evidence management, industry-standard computer forensic tools, file systems, data recovery and collection and sample case evaluations. Each student is required to sign an ethical agreement with the instructor.

CIT 181 Principles of Information Security 4 credits

(Prerequisite: CIT-115 or instructor approval)

This course provides students necessary background in the technical realities and legal and theoretical principles of computer and information security to help them identify and evaluate computer security crimes and incidents. Topics include information security components and models, legal and ethical issues in information security and privacy, basics of computer networks and data communication, common computer and network system threats, attacks and vulnerabilities, as well as information security risk and damage analysis and assessment.

CIT 185 Network Security 3 credits
(Prerequisite: CIT-175)
This course highlights the models and protocols essential to securing wired and wireless networks. Students also learn to capture and analyze network traffic, identify network security threats, and apply and evaluate network security controls.

CIT 186 Intrusion Detection and Prevention 3 credits
(Prerequisite: CIT-175)
This course covers the basic theory and practice of detecting and preventing intrusions and attacks in cyberspace. The study emphasis is on methods and tools to monitor for and identify system vulnerabilities and threats and prevent attacks.

CIT 282 Advanced Cybersecurity Topics 3 credits
(Prerequisite: CIT-185)
This course covers advanced and emerging topics in Cybersecurity. The current emphasis in the course is on mobile device security and cloud security.

CIT 285 Cybersecurity Capstone 3 credits
(Prerequisite: Instructor approval)
This course, which must be taken in the final semester, is the exit course for the program. With the instructor's guidance and approval, each student will work on and complete a portfolio-type project on a specific cybersecurity problem using the learning from previous courses in the program and additional research.