**Mission**

Provide students with essential conceptual knowledge and skills to prevent, investigate, and enforce cybercrimes and cyberthreats. This program combines elements of law enforcement, computer investigative, legal, and security skills, forensics, and other related fields in the study of crime prevention and response to various crimes occurring in the cyber world. Graduates of the program will be well prepared for traditional and emerging positions related to prevention, investigation, and enforcement of crime generally, and cyber-related crimes more specifically.

**Program Learning Outcomes**

1. Gain conceptual knowledge and technological skills necessary in the detection, investigation, and enforcement of cybercrimes
2. Understand the multitude of issues, theories, ethics, policies, practices, and current challenges related to the control of cybercrime
3. Develop an understanding of how traditional criminal justice theories, practices, and policies, and cybersecurity tools, techniques and technologies apply to the control of cybercrime

**Core Courses**

**Criminal Justice**

* CJ 213 Introduction to Criminal Justice **Credits: 4**
* CJ 331 Police and Community **Credits: 4**
* CJ 352 Criminal Law **Credits: 4**
* CJ 452 Criminal Procedure **Credits: 4**

**Cybercrime Investigation and Enforcement**

* CIE 213 Introduction to Cybercrime **Credits: 4**
* CIE 305 Ethics in Cybercrime Investigation and Enforcement **Credits: 4**
* CIE 321 Principles of Cyber Forensic Investigations **Credits: 4**
* CIE 425 Contemporary Issues on Cybercrime and Cybersecurity **Credits: 4**
* CIE 407 Capstone Seminar **Credits: 4**
* CIE 409 Practicum **Credits: 4**

**Information Systems**

* IS 283 Cybersecurity Fundamentals **Credits: 4**
* IS 373 Computer Security **Credits: 4**
* IS Network Security **Credits: 4**
* IS 474 Ethical Hacking **Credits: 4**

**Choose Four**

* Upper division courses from CJ, CIE or IS, this may include an additional 4 credits of CIE 409.

**Total Credits 72**