CCT 110 Introduction to Cybercrime

COURSE DESCRIPTION:

Prerequisites: None

Corequisites: None

This course examines various cybercrime types, digital forensic investigation techniques, and the ethical dilemmas posed by technology and cyber offenses. Students will learn about the technical aspects of cybercrime, legal frameworks, and ethical considerations, preparing them to make informed decisions in their future cybersecurity careers.

Course Hours per Week: Class, 3. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completing requirements for this course, the student will be able to:

1. Analyze various types of cybercrime and understand the methodologies employed by cyber criminals and their technological foundations.
2. Discuss and evaluate the ethical implications of cybercrime and cybersecurity practices on privacy and civil liberties.
3. Develop strategies for preventing cybercrime and protecting digital assets in organizational contexts.
4. Critically assess cybercrime policy and legislation from a technological perspective.
5. Apply best practices and digital forensic techniques to investigate and mitigate cybercrime incidents.

OUTLINE OF INSTRUCTION:

I. Cybercrime Fundamentals and IT Perspectives
   A. Overview of cybercrime: Types, trends, and technological roots.
   B. The role of IT professionals in combating cybercrime.

II. Technical Deep Dive into Cyber Offenses
   A. Computer hacking, malware analysis, and defense strategies.
   B. Digital piracy, intellectual property theft, and prevention techniques.

III. Cybercrime Against Individuals and Organizations
   A. Protecting against online fraud, phishing, and economic crimes.
   B. Strategies for IT professionals to combat cyber-bullying, cyber-stalking.

IV. Digital Forensics and Incident Response
   A. Investigating Cybercrime
   B. Introduction to digital forensics tools and methodologies.
   C. Role of IT in legal considerations and incident response planning.

V. Ethics, Policy, and the Future of Cybercrime
   A. Ethical dilemmas in cybersecurity: surveillance, hacking back.
   B. Cybercrime policy and the IT professional's role in shaping legislation.

C. Overview of cybercrime: Types, trends, and technological roots.
D. The role of IT professionals in combating cybercrime.

VI. Technical Deep Dive into Cyber Offenses
A. Computer hacking, malware analysis, and defense strategies.
B. Digital piracy, intellectual property theft, and prevention techniques.

VII. Cybercrime Against Individuals and Organizations
A. Protecting against online fraud, phishing, and economic crimes.
B. Strategies for IT professionals to combat cyber-bullying, cyber-stalking.

VIII. Digital Forensics and Incident Response
A. Investigating Cybercrime
B. Introduction to digital forensics tools and methodologies.
C. Role of IT in legal considerations and incident response planning.

IX. Ethics, Policy, and the Future of Cybercrime
A. Ethical dilemmas in cybersecurity: surveillance, hacking back.
B. Cybercrime policy and the IT professional's role in shaping legislation.

REQUIRED TEXTBOOK AND MATERIAL:

The textbook and other instructional material will be determined by the instructor.