CIS 170 – Information Technology in Criminal Justice

Course Description

This course examines how information technology is used within the criminal justice system, Homeland Security, and private security. Topics covered include information systems and communication technologies used to prevent and investigate crime and manage security. Students will develop fundamental technical and research skills applicable to criminal justice.

Instructional Materials

Taylor, R., Fritsch, E. J., Liederbach, J., Holt, T. J. (2011). *Digital crime, digital terrorism* (2nd ed.). Upper Saddle River, NJ: Pearson.

Course Learning Outcomes

1. Explain digital crime and digital terrorism activities.
2. Describe law enforcement roles and responses.
3. Identify information system attacks and countermeasures.
4. Describe the criminology of computer crime.
5. Analyze the types of digital criminals and hackers.
6. Summarize white-collar crimes and criminal tools.
7. Explain computer viruses and malicious computer code.
8. Analyze the different types of crimes on the World Wide Web involving victimization, sex crimes, and obscenity.
9. Explain the various digital laws and legislation in support of law enforcement.
10. Explain the procedures in the investigation of computer-related crime.
11. Describe the technologies and processes involved in digital forensics.
12. Describe future trends in digital crime and terrorism.
13. Evaluate the ethical concerns that information technologies raise in society and the impact of information technologies on crime, terrorism, or war.
14. Use technology and information resources to research issues in information technology in criminal justice.
15. Write clearly and concisely about information technology in criminal justice topics using proper writing mechanics and technical style conventions.