

CIS 324 – Computer Ethics

Course Description

This course provides critical ethical and legal information that computer security professional must take into account when developing security policies, plans, and procedures. This course focuses on ethical and legal issues and privacy considerations that organizations must take into account. Topics also include issues related to risk mitigation and analysis, incidence response and contingency planning.

Instructional Materials

Grams, J. L., (2011). *Legal Issues in Information Security*. Jones and Bartlett.

Course Learning Outcomes

1. Summarize the legal aspects of the information security triad: availability, integrity, and confidentiality.
2. Explain the concept of privacy and its legal protections.
3. Describe the basic components of the American Legal System.
4. Describe legal compliance laws addressing public and private institutions.
5. Analyze intellectual property laws.
6. Differentiate the role of contracts in online transactions and cyberspace.
7. Identify cybercrime and tort law, and ethical issues in cyberspace.
8. Examine the principles requiring governance of information within organizations.
9. Identify risk analysis and incident response procedures.
10. Explain the importance of forensics examination in legal proceedings.
11. Use technology and information resources to research legal issues in information security.
12. Write clearly and concisely about information security legal issues and topics using proper writing mechanics and technical style conventions.