California State University, Northridge
College of Business & Economics
Department of Accounting & Information Systems

IS 497B: Information Security and Assurance
Reading Preparation Assignment
Management of Information Security
Chapter 12

Read Chapter 12, Law and Ethics, of the *Management of Information Security* textbook, pp. 445-483.

The following review questions will be used to lead class discussion.

1. What is the difference between criminal law and civil law?
2. What is tort law and what does it permit an individual to do?
3. What are the three primary types of public law?
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
5. What is privacy in the context of information security?
6. Why is the Kennedy-Kassebaum Act of 1996 (a.k.a. HIPPA) important to organizations that are not in the health care industry?
7. If you work for a financial service organization (such as a bank or credit union), which law from 1999 affects your use of customer data? What other effects does it have?
8. Which 1997 law provides guidance on the use of encryption?
9. What is intellectual property? Is it offered the same protection in every country? What laws currently protect intellectual property in the United States and Europe?
10. How does policy differ from a law?
11. What are the three general categories of unethical and illegal behavior?
12. What is the best method for preventing illegal or unethical behavior?
13. Of the professional organizations discussed in this chapter, which is focused on auditing and control?
14. What is the primary mission of the Information Systems Security Association?
15. What is the stated purpose of the SANS organization? In what ways is it involved in professional certification for InfoSec professionals?
16. Which U.S. federal agency sponsors the InfraGard program? Which agency has taken control of the overall National Infrastructure Protection mission?
17. What is due care? Why would an organization want to make sure it exercises due care in its usual course of operations?
18. What should an organization do to deter someone from violating policy or committing a crime?
19. How does due diligence differ from due care? Why are both important?