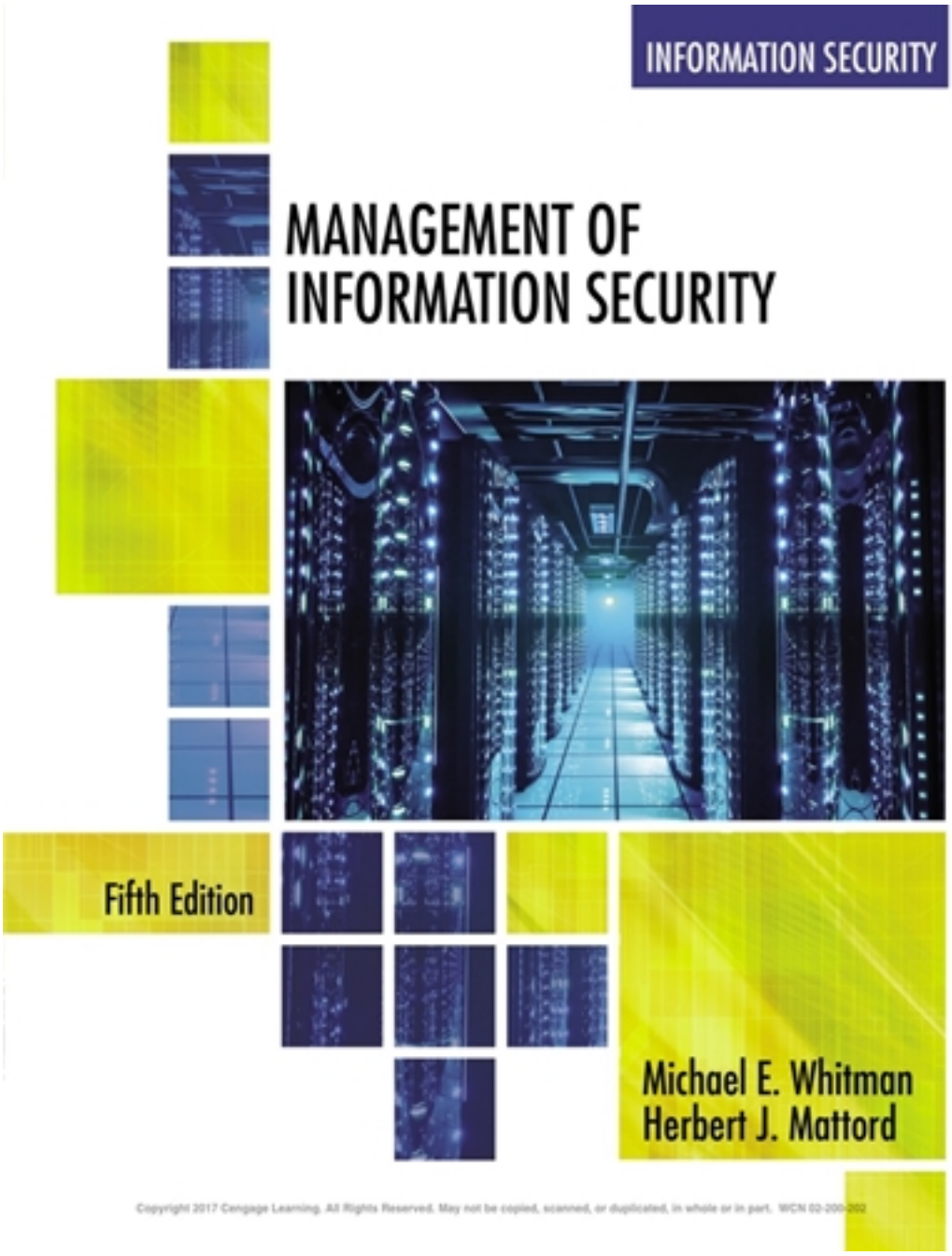
Test Bank for Management of Information Security 5th Edition by Whitman

CLICK HERE TO ACCESS COMPLETE Test Bank



Test Bank

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

1. Ethics carry the sanction of a governing authority.
   a. True
   b. False

ANSWER: False
POINTS: 1
REFERENCES: InfoSec and the Law
QUESTION TYPE: True / False
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 2:43 PM

2. The Secret Service is charged with the detection and arrest of any person committing a U.S. federal offense relating to computer fraud, as well as false identification crimes.
   a. True
   b. False

ANSWER: True
POINTS: 1
REFERENCES: Key Law Enforcement Agencies
QUESTION TYPE: True / False
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 3:27 PM

3. Deterrence is the best method for preventing an illegal or unethical activity. _____
ANSWER: True
POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:59 PM
DATE MODIFIED: 2/24/2016 5:59 PM

4. ISACA is a professional association with a focus on authorization, control, and security. _____
ANSWER: False - auditing
POINTS: 1
REFERENCES: Information Systems Audit and Control Association (ISACA)
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 6:00 PM
DATE MODIFIED: 2/24/2016 6:01 PM

5. Due diligence requires that an organization make a valid and ongoing effort to protect others. _____
ANSWER: True

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

POINTS: 1
REFERENCES: Organizational Liability and the Need for Counsel
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 6:02 PM
DATE MODIFIED: 2/24/2016 6:02 PM

6. The Gramm-Leach-Bliley (GLB) Act (also known as the Financial Services Modernization Act of 1999) contains a number of provisions that affect banks, securities firms, and insurance companies. _____
ANSWER: True
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:52 PM
DATE MODIFIED: 2/24/2016 6:20 PM

7. It is the responsibility of InfoSec professionals to understand state laws and standards. _____
ANSWER: False - regulations
POINTS: 1
REFERENCES: State and Local Regulations
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:57 PM
DATE MODIFIED: 2/24/2016 5:58 PM

8. InfraGard began as a cooperative effort between the FBI's Cleveland field office and local intelligence professionals. _____
ANSWER: False - technology
POINTS: 1
REFERENCES: Key Law Enforcement Agencies
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 6:04 PM
DATE MODIFIED: 2/24/2016 6:05 PM

9. Information ambiguation occurs when pieces of non-private data are combined to create information that violates privacy. _____

ANSWER: False - aggregation
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Modified True / False

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:43 PM
DATE MODIFIED: 2/24/2016 5:47 PM

10. To protect intellectual property and competitive advantage, Congress passed the Entrepreneur Espionage Act (EEA) in 1996. _____
ANSWER: False - Economic
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:55 PM
DATE MODIFIED: 3/21/2016 9:24 PM

11. A signaling law specifies a requirement for organizations to notify affected parties when they have experienced a specified type of loss of information. _____
ANSWER: False - breach
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
DATE CREATED: 2/24/2016 5:48 PM
DATE MODIFIED: 2/24/2016 5:55 PM

12. Which subset of civil law regulates the relationships among individuals and among individuals and organizations?
a. tort b. criminal
c. private d. public
ANSWER: c
POINTS: 1
REFERENCES: Types of Law
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:16 PM

13. Which law addresses privacy and security concerns associated with the electronic transmission of PHI?
a. USA Patriot Act of 2001
b. American Recovery and Reinvestment Act
c. Health Information Technology for Economic and Clinical Health Act
d. National Information Infrastructure Protection Act of 1996
ANSWER: c
POINTS: 1
REFERENCES: Relevant U.S. Laws

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:18 PM

14. The penalties for offenses related to the National Information Infrastructure Protection Act of 1996 depend on whether the offense is judged to have been committed for one of the following reasons except which of the following?

a. For purposes of commercial advantage
b. For private financial gain
c. For political advantage
d. In furtherance of a criminal act

ANSWER: c
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:20 PM

15. Which law requires mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system?

a. The Telecommunications Deregulation and Competition Act
b. National Information Infrastructure Protection Act
c. Computer Fraud and Abuse Act
d. The Computer Security Act

ANSWER: d
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:21 PM

16. Which act is a collection of statutes that regulates the interception of wire, electronic, and oral communications?

a. The Electronic Communications Privacy Act of 1986
b. The Telecommunications Deregulation and Competition Act of 1996
c. National Information Infrastructure Protection Act of 1996
d. Federal Privacy Act of 1974

ANSWER: a
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:22 PM

17. Which act requires organizations that retain health care information to use InfoSec mechanisms to protect this information, as well as policies and procedures to maintain them?

a. ECPA
b. Sarbanes-Oxley
c. HIPAA
d. Gramm-Leach-Bliley

ANSWER: c
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:28 PM

18. Which law extends protection to intellectual property, which includes words published in electronic formats?

a. Freedom of Information Act
b. U.S. Copyright Law
c. Security and Freedom through Encryption Act
d. Sarbanes-Oxley Act

ANSWER: b
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:27 PM

19. Which of the following is the study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences and is also known as duty- or obligation-based ethics?

a. Applied ethics
b. Meta-ethics
c. Normative ethics
d. Deontological ethics

ANSWER: d
POINTS: 1
REFERENCES: Ethics in InfoSec
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:30 PM

20. Which of the following is an international effort to reduce the impact of copyright, trademark, and privacy infringement, especially via the removal of technological copyright protection measures?

a. U.S. Copyright Law

Name:_____ Class:_____ Date:_____

b. PCI DSS
c. European Council Cybercrime Convention
d. DMCA

ANSWER: d
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:32 PM

21. Which of the following ethical frameworks is the study of the choices that have been made by individuals in the past; attempting to answer the question, what do others think is right?

a. Applied ethics b. Descriptive ethics
c. Normative ethics d. Deontological ethics

ANSWER: b
POINTS: 1
REFERENCES: Ethics in InfoSec
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:33 PM

22. Which ethical standard is based on the notion that life in community yields a positive outcome for the individual, requiring each individual to contribute to that community?

a. utilitarian b. virtue
c. fairness or justice d. common good

ANSWER: d
POINTS: 1
REFERENCES: Ethics in InfoSec
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:34 PM

23. There are three general categories of unethical behavior that organizations and society should seek to eliminate. Which of the following is NOT one of them?

a. ignorance b. malice
c. accident d. intent

ANSWER: b
POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Multiple Choice

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:35 PM

24. Which of the following is the best method for preventing an illegal or unethical activity? Examples include laws, policies and technical controls.

a. remediation b. deterrence
c. persecution d. rehabilitation

ANSWER: b
POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:36 PM

25. Which of the following organizations put forth a code of ethics designed primarily for InfoSec professionals who have earned their certifications? The code includes the canon: Provide diligent and competent service to principals.

a. $(ISC)^2$ b. ACM
c. SANS d. ISACA

ANSWER: a
POINTS: 1
REFERENCES: International Information Systems Security Certification Consortium, Inc. (ISC)2
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:38 PM

26. Which of the following is compensation for a wrong committed by an employee acting with or without authorization?

a. liability b. restitution
c. due diligence d. jurisdiction

ANSWER: b
POINTS: 1
REFERENCES: Organizational Liability and the Need for Counsel
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 3/21/2016 9:24 PM

27. Any court can impose its authority over an individual or organization if it can establish which of the following?

a. jurisprudence b. jurisdiction
c. liability d. sovereignty

ANSWER: b

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

POINTS: 1
REFERENCES: Organizational Liability and the Need for Counsel
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:57 PM

28. _____ is a subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury.
ANSWER: tort law
POINTS: 1
REFERENCES: Types of Law
QUESTION TYPE: Completion
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:54 PM

29. Ethics are based on _____, which are the relatively fixed moral attitudes or customs of a societal group.
ANSWER: cultural mores
POINTS: 1
REFERENCES: InfoSec and the Law
QUESTION TYPE: Completion
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 4:59 PM

30. An organization increases its _____ if it refuses to take measures—due care—to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions.
ANSWER: liability
POINTS: 1
REFERENCES: 476
QUESTION TYPE: Completion
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:00 PM

31. Information _____ occurs when pieces of non-private data are combined to create information that violates privacy.
ANSWER: aggregation
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Completion
HAS VARIABLES: False

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

DATE CREATED: 2/24/2016 6:08 PM
DATE MODIFIED: 2/24/2016 6:10 PM

32. The act of attempting to prevent an unwanted action by threatening punishment or retaliation on the instigator if the act takes place is known as _____.
ANSWER: deterrence
POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Completion
HAS VARIABLES: False
DATE CREATED: 2/24/2016 6:13 PM
DATE MODIFIED: 2/24/2016 6:13 PM

33. The branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment is known as _____.
ANSWER: ethics
POINTS: 1
REFERENCES: Ethics in InfoSec
QUESTION TYPE: Completion
HAS VARIABLES: False
DATE CREATED: 2/24/2016 6:11 PM
DATE MODIFIED: 2/24/2016 6:11 PM

34. Briefly describe five different types of laws.
ANSWER: 1. Civil law embodies a wide variety of laws pertaining to relationships between and among individuals and organizations.
2. Criminal law addresses violations harmful to society and is actively enforced and prosecuted by the state.
3. Tort law is a subset of civil law which allows individuals to seek recourse against others in the event of personal, physical, or financial injury.
4. Private law regulates the relationships among individuals and among individuals and organizations, and encompasses family law, commercial law, and labor law.
5. Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.
POINTS: 1
REFERENCES: Types of Law
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:12 PM

35. Discuss the three general categories of unethical behavior that organizations should try to control.
ANSWER: Ignorance:
Ignorance of the law is no excuse, but ignorance of policies and procedures is. The first method of deterrence is education. Organizations must design, publish, and disseminate organizational policies

and relevant laws, and employees must explicitly agree to abide by them. Reminders, training, and awareness programs support retention, and one hopes, compliance.
Accident:
Individuals with authorization and privileges to manage information within the organization have the greatest opportunity to cause harm or damage by accident. The careful placement of controls can help prevent accidental modification to systems and data.
Intent:
Criminal or unethical intent refers to the state of mind of the individual committing the infraction. A legal defense can be built upon whether or not the accused acted out of ignorance, by accident, or with the intent to cause harm or damage. Deterring those with criminal intent is best done by means of litigation, prosecution, and technical controls. Intent is only one of several factors to consider when determining whether a computer-related crime has occurred.

POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:13 PM

36. Laws and policies and their associated penalties only deter if three conditions are present. What are these conditions?
ANSWER: Fear of penalty—Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
Probability of being caught—There must be a strong possibility that perpetrators of illegal or unethical acts will be caught.
Probability of penalty being administered—The organization must be willing and able to impose the penalty.
POINTS: 1
REFERENCES: Deterring Unethical and Illegal Behavior
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:34 PM

37. What is the key difference between law an ethics?
ANSWER: The key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not.
POINTS: 1
REFERENCES: Policy Versus Law
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:36 PM

38. The penalty for violating the National Information Infrastructure Protection Act of 1996 depends on the value of the information obtained and whether the offense is judged to have been committed for one of three reasons. What are those reasons?

Name:_____ Class:_____ Date:_____

ANSWER: For purposes of commercial advantage
For private financial gain
In furtherance of a criminal act
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:38 PM

39. The Computer Security Act charges the National Bureau of Standards, in cooperation with the National Security Agency (NSA), with the development of five standards and guidelines establishing minimum acceptable security practices. What are three of these principles?

ANSWER: Standards, guidelines, and associated methods and techniques for computer systems
Uniform standards and guidelines for most federal computer systems
Technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems
Guidelines for use by operators of federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice
Validation procedures for, and evaluation of the effectiveness of, standards and guidelines through research and liaison with other government and private agencies
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 3/21/2016 9:25 PM

40. Describe the Freedom of Information Act. How does its application apply to federal vs. state agencies?

ANSWER: All federal agencies are required under the Freedom of Information Act (FOIA) to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records.
POINTS: 1
REFERENCES: Relevant U.S. Laws
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:40 PM

41. A key difference between policy and law is that ignorance of policy is a viable defense. What steps must be taken to assure that an organization has a reasonable expectation that policy violations can be appropriately penalized without fear of legal retribution?

ANSWER: Policies must be:

Distributed to all individuals who are expected to comply with them
Read by all employees
Understood by all employees, with multilingual translations and translations for visually impaired or low-literacy employees
Acknowledged by the employee, usually by means of a signed consent form
Uniformly enforced, with no special treatment for any group (e.g., executives)

POINTS: 1
REFERENCES: Policy Versus Law
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 3/21/2016 9:26 PM

42. Describe three of the five foundations and frameworks of ethics.

ANSWER: Normative ethics—The study of what makes actions right or wrong, also known as moral theory—that is, how should people act?
Meta-ethics—The study of the meaning of ethical judgments and properties—that is, what is right?
Descriptive ethics—The study of the choices that have been made by individuals in the past—that is, what do others think is right?
Applied ethics—An approach that applies moral codes to actions drawn from realistic situations; it seeks to define how we might use ethics in practice.
Deontological ethics—The study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences; also known as dutybased or obligation-based ethics. This approach seeks to define a person's ethical duty.

POINTS: 1
REFERENCES: Ethics in InfoSec
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 2/24/2016 5:42 PM

a. criminal law
b. public law
c. ethics
d. Computer Security Act (CSA)
e. Electronic Communications Privacy Act
f. Cybersecurity Act
g. normative ethics
h. applied ethics

REFERENCES: 454
462
467
479
456

Name:_____ Class:_____ Date:_____

Chapter 02: Compliance: Law and Ethics

447
QUESTION TYPE: Matching
HAS VARIABLES: False
DATE CREATED: 2/22/2016 4:25 PM
DATE MODIFIED: 3/21/2016 9:27 PM

43. one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices
ANSWER: d
POINTS: 1

44. focuses on enhancing the security of the critical infrastructure in the United States
ANSWER: f
POINTS: 1

45. an approach that applies moral codes to actions drawn from realistic situations
ANSWER: h
POINTS: 1

46. a collection of statutes that regulates the interception of wire, electronic, and oral communications

ANSWER: e
POINTS: 1

47. regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments
ANSWER: b
POINTS: 1

48. the study of what makes actions right or wrong, also known as moral theory
ANSWER: g
POINTS: 1

49. addresses violations harmful to society and is actively enforced and prosecuted by the state
ANSWER: a
POINTS: 1

50. defines socially acceptable behaviors
ANSWER: c
POINTS: 1