Multiple-Choice Questions

1. **Which of the following statements best defines *computer ethics*?**

   o   A) The study of how computers function in business

   o   B) Guidelines that inform acceptable use of information technology

   o   C) Rules for purchasing computer equipment

   o   D) Standards for software development

Answer: B

2. **Which factor has *not* contributed to the rise in computer-related security incidents?**

   o   A) Increasing complexity of IT systems

   o   B) Higher user expectations for convenience

   o   C) Limited storage capabilities of modern devices

   o   D) Expanding and changing systems in organizations

Answer: C

3. **What is the main role of *compliance* in a business setting?**

   o   A) To increase profit margins

   o   B) To ensure adherence to legal and ethical standards

   o   C) To minimize employee workload

   o   D) To create new IT projects

Answer: B

4. **In an ethical business context, *integrity* refers to:**

   o   A) Following all business policies strictly, regardless of context

   o   B) Acting according to one's personal beliefs in all situations

   o   C) Adhering to a personal code of principles consistently

   o   D) Avoiding complex situations to prevent moral dilemmas

Answer: C

5. **Which of the following practices is an example of an *ethical IT behavior*?**

   o   A) Using company resources for personal projects

   o   B) Reporting a security vulnerability to a manager

   o   C) Ignoring a client's request for a progress update

- o D) Sharing confidential information with friends

Answer: B

6. **Which of the following is a *primary benefit* of implementing strong corporate ethics?**

   - o A) Reduced operating costs

   - o B) Enhanced reputation and trust among stakeholders

   - o C) Reduced software maintenance requirements

   - o D) Simplified internal reporting systems

Answer: B

7. **What does the term *multilayered security* refer to in IT security?**

   - o A) Using multiple types of encryption for the same data

   - o B) Employing various levels of security measures to protect information

   - o C) Implementing security in different company departments

   - o D) Having redundant security staff for each area

Answer: B

8. **Which of the following is an example of *conflict of interest* for an IT worker?**

   - o A) Recommending additional training for IT staff

   - o B) Promoting products from a company in which they own shares

   - o C) Reporting unethical behavior to management

   - o D) Attending a company-sponsored ethics training session

Answer: B

9. **An *ethical dilemma* typically involves which of the following?**

   - o A) Choosing between two right actions

   - o B) Choosing between right and wrong actions

   - o C) A straightforward business decision

   - o D) Any technical problem with a simple solution

Answer: A

10. **Which of the following best defines *phishing*?**

   - o A) A type of malware designed to lock users out of their systems

   - o B) The use of fake messages to trick people into providing confidential information

- o C) Scanning a network for security vulnerabilities

- o D) The illegal copying of software

Answer: B

True/False Questions

1. **T/F:** IT professionals have a duty to disclose any potential conflicts of interest.

    - o *Answer: True*

2. **T/F:** Misusing company resources, such as using software for personal gain, is considered an unethical behavior.

    - o *Answer: True*

3. **T/F:** The *Digital Millennium Copyright Act (DMCA)* is designed to protect the privacy of individuals on social media.

    - o *Answer: False* (It protects intellectual property rights.)

4. **T/F:** All IT workers are legally bound by professional codes of ethics in their field.

    - o *Answer: False* (Not all IT roles are recognized as professional positions with mandatory ethics codes.)

5. **T/F:** An organization's commitment to ethics has no effect on employee morale or retention.

    - o *Answer: False* (Good ethics often positively impact morale and retention.)

6. **T/F:** Failing to report a data breach to affected customers could damage a company's reputation and violate legal obligations.

    - o *Answer: True*

7. **T/F:** A company known for its corporate social responsibility (CSR) practices may attract more loyal customers.

    - o *Answer: True*

8. **T/F:** IT systems that operate in cloud environments require less attention to data security than in-house systems.

    - o *Answer: False* (Cloud environments require rigorous security practices.)

9. **T/F:** The Sarbanes-Oxley Act of 2002 was established to improve financial reporting and prevent accounting scandals in the U.S.

    - o *Answer: True*

10. **T/F:** If an IT professional observes a significant ethical violation by another employee, they are ethically obligated to report it, even if it could negatively impact them personally.

- *Answer: True*

Additional Multiple-Choice Questions

11. **The term *reasonable assurance* in IT security refers to:**

    - A) Ensuring complete immunity to security breaches

    - B) Implementing measures to reasonably protect against risks within practical limits

    - C) Using an extensive set of security measures to eliminate all threats

    - D) Guaranteeing that no security incidents will occur

Answer: B

12. **Which of the following is typically included in a company's code of ethics?**

    - A) Guidelines for employee behavior

    - B) Instructions for software installation

    - C) Detailed financial targets

    - D) Policies for vacation and leave

Answer: A

13. **What is the main objective of *ethical decision-making*?**

    - A) To follow orders from supervisors

    - B) To achieve the best outcome within moral, ethical, and legal frameworks

    - C) To ensure projects are completed under budget

    - D) To enhance technical efficiency in all projects

Answer: B

14. **Which of the following is a common method for promoting ethical behavior among employees?**

    - A) Reducing employee benefits

    - B) Providing ethics training and guidelines

    - C) Allowing employees to set their own rules

    - D) Limiting access to professional development

Answer: B

15. **Why is it important for organizations to conduct *regular security audits*?**

- A) To guarantee security breaches won't happen

- B) To verify the effectiveness of security measures and compliance

- C) To ensure all employees are working at full capacity

- D) To prevent the need for backup systems

Answer: B