UNIVERSITY OF GHANA

BSc. FIRST SEMESTER UNIVERSITY EXAMINATIONS: 2017/2018

DEPARTMENT OF COMPUTER SCIENCE

CSIT 201: PROFESSIONAL, LEGAL MORAL AND ETHICAL ISSUES IN INFORMATION TECHNOLOGY (3 CREDITS)

NATIONAL:

Answer ALL questions in Section A and any THREE questions in Section B

TIME ALLOWED: 2 HOURS

SECTION A

ANSWER ALL QUESTIONS IN THIS SECTION - [40 MARKS]

Please circle or write down the most appropriate option in the following questions.

1. A suite of guiding beliefs, standards, or ideals that pervades an individual, group, or community of people is:
    a. Ethics
    b. Morals
    c. Integrity
    d. Laws

2. Which of the following is not a reason a business engages in business ethics?
    a. To recover a company's image after a notorious business scandal
    b. To avoid the loss of a good corporate image or being sued for misconduct
    c. To enhance global relationships
    d. To act with real commitment

3. Two major conflicting issues related to privacy are ___ and ___
    a. Freedom of speech, human rights
    b. Human rights, equal opportunity employment
    c. Freedom of speech, national security
    d. None of these

EXAMINER: DR FERDINAND A. KATSRIKU

4. A .... is a form of protection for intellectual property that does not require any disclosure or the filing of an application.
   a. copyright
   b. patent
   c. trade secret
   d. trademark

5. Rules of conduct or actions recognized by customs or decreed by a formal body and enforceable by some instrument is........
   a. Moral codes
   b. Law
   c. Moral standards
   d. Conscience

6. .... broadly describes tangible things such as ideas, inventions, technologies, artworks, music and literature, and others that one can claim ownership to
   a. Intellectual property
   b. Professional Ethics
   c. Laws
   d. Character

7. ……………. is a system of set rules prescribing punishment for unlawful acts.
   a. Natural law
   b. Conventional law
   c. Ethical law
   d. The Penal Code.

8. .... includes relationships with and responsibilities toward customers, clients, coworkers, employees, employers, others who use one's products and services.
   a. Morals
   b. Professional ethics
   c. Laws
   d. Character

9. A.......... is an expert in a field:
   a. professional
   b. Morals
   c. Integrity
   d. Laws

10. .... provide a general statement of ethical values:
    a. professional
    b. Professional Codes of Ethics
    c. Integrity
    d. Laws

11. .... and the Internet make copyright infringement easier and cheaper.

a. professional systems
b. Digital technology
c. Copyright technology
d. Software piracy

12. The written statement that defines an organization's security requirements as well as the controls and sanctions used to meet those requirements is known as a:
   a. risk assessment
   b. security policy
   c. firewall
   d. none of the above

13. .... is a form of malware that, if a user unknowingly downloads it to his or her smartphone, takes control of the device and its data until the owner agrees to pay a ransom to the attacker.
   a. virus
   b. bacteria
   c. ransomware
   d. Trojan

14. .... is the application of forensic science investigative techniques to computer-based material used as evidence.
   a. man-in-the-middle
   b. metaspliot
   c. Safe Harbor
   d. Computer Forensics

15. A piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.

   a. botnet

   b. phishing

   c. Bring your own device (BYOD)

   d.virus

16. The act of fraudulently using email to try to get the recipient to reveal personal data.

   Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
   phishing
   cracker
   Bring your own device (BYOD)

17. Software that generates and grades tests that humans can pass but all but the most sophisticated computer programs cannot.

   a. antivirus software

b. CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)

c. US Cert - computer emergency readiness team

d. zombie

18. A program in which malicious code is hidden inside a seemingly harmless program.

    a. virus

    b. industrial spy

    c. Trojan horse

    d. phishing

19. An attack on an information system that takes advantage of a particular system vulnerability. (worms, Trojans, phishing, rootkit, etc.)

    a. computer fraud and abuse act

    b. exploit

    c. zero-day attack

    d. distributed denial-of-service attack (DDoS)

20. A calling that requires specialized knowledge and often long and intensive academic preparation.

    a. Profession

    b. certification

    c. negligence

    d. professional malpractice

21. A statement of the principles and core values that are essential to the work of a particular occupational group.

    a. professional code of ethics

    b. Foreign Corrupt Practices Act (FCPA)

    c. professional malpractice

    d. profession

22. An effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.

    a. negligence

    b. body of knowledge

    c. whistle-blowing

    d. certification

23. A government-issued permission to engage in an activity or to operate a business; it is generally administered at the state level and often requires that the recipient pass a test of some kind.

    a. certification

    b. trade secret

    c. body of knowledge

    d. government license

24. An agreed-upon set of skills and abilities that all licensed professionals in a particular type of profession must possess.

    a. whistle-blowing

    b. duty of care

    c. certification

    d. body of knowledge

25. An approach to ethical decision making based on a vision of society as a community whose members work together to achieve a common set of values and goals.

    a. virtue ethics approach

    b. utilitarian approach

    c. fairness approach

    d. common good approach

26. One's personal beliefs about right and wrong.

    a. morality

    b. virtue

    c. ethics

    d. morals

In the following questions indicate whether or the statement is TRUE or FALSE

27. A 2004 law that specifies requirements that commercial emailers must follow when sending out messages that advertise or promote a commercial product or service is called Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act

    True   False

28. An individual, motivated by the potential for monetary gain, who hacks into computers to steal, often by transferring money from one account to another to another is referred to as US Cert - computer emergency readiness team

   True   False

29. A concept in computer security that recognizes that managers must use their judgment to ensure that the cost of control does not exceed the system's benefits or the risks involved is referred to as reasonable assurance

   True   False

30. An individual who launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives is referred to as cyberterrorist

   True   False

31. A written statement that defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements is called security policy

True False

In the following questions, find a word or phrase that correctly describes each of the following:

32. A poorly trained and inadequately managed employee who means well but who has the potential to cause much damage.

   _____

33. A type of Trojan horse that executes when it is triggered by a specific event.

   _____

34. Hacking to achieve a political or social goal.

   _____

35. A specific sequence of bytes that indicates to antivirus software that a specific virus is present.

   _____

36. A discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered so it is admissible as evidence in a court of law.

   _____

37. A variation of phishing in which victims receive a voicemail telling them to call a specific phone number or log on to access a specific Web site.

   _____

38. A harmful program that resides in the active memory of a computer and duplicates itself.

   _____

39. An attack that takes place before the security community or software developer knows about the vulnerability or has been able to repair it.

_____

40. A computer that is part of a botnet and that is controlled by a hacker without the knowledge or consent of its owner.

_____

SECTION B [60 MARKS]

<u>*ANSWER ANY THREE QUESTIONS FROM THIS SECTION – 20 MARKS EACH*</u>

<u>Question B1</u>   [*20 Marks*]

a.   What is ethics, and why is it important to act according to a code of ethics?   5 Marks

b.   Why is business ethics becoming increasingly important?   5 Marks

c.   What are organizations doing to improve their business ethics?   5 Marks

d. Describe a hypothetical situation in which the action you would take is not legal, but it is ethical. Describe a hypothetical situation where the action you would take is legal, but not ethical. 5 Marks

<u>Question B2</u>   [*20 Marks*]

a.   What impact has IT had on the standard of living and worker productivity?   4Marks

b.   Define the term telework. What technologies are essential for effective telework?   4Marks

c.   Would you accept a telework position in which you would work from home three or four days per week? Why or why not?
       4Marks

d.   What is the digital divide? Where does it exist? Why is it important to bridge the digital divide?

      8Marks

<u>Question B3</u>   [*20 Marks*]

a.   What are the most common types of computer security attacks?   4Marks

b.   Who are the primary perpetrators of computer crime, and what are their objectives?   4Marks

c.   What is computer forensics? In addition to computer-related training, what other education and

EXAMINER: DR FERDINAND A. KATSRIKU

background would be ideal for someone who wants to make a career in computer forensics?

4Marks

d. Some IT security personnel believe that their organizations should employ former computer criminals to identify weaknesses in their organizations' security defenses. Do you agree? Why or why not?   8 Marks

Question B4   [*20 Marks*]

 a. Discuss briefly the social problems of online social networks.   5 Marks
b. Briefly explain the difference between risk assessment and an IT security audit?   5 Marks
c. Briefly discuss strategies that can be used to effectively eliminate online social network crimes.   5 Marks
d. Explain the concept that an idea cannot be copyrighted, but the expression of an idea can be, and why this distinction is a key to understanding copyright protection?   5 Marks