STUDENT'S ID.NO:_____ SIGNATURE: _____

UNIVERSITY OF GHANA
(All rights reserved)
DEPARTMENT OF TEACHER EDUCATION
SCHOOL OF EDUCATION AND LEADERSHIP
COLLEGES OF EDUCATION
END OF YEAR FOUR SEMESTER TWO EXAMINATIONS, 2023/2024
B.ED. PROGRAMME

COURSE: LEGAL AND SECURITY ISSUES IN ICT
COURSE CODE: TEJS 406

Instruction: Answer all questions in Section A and any three in Section B.

Time: 2 hours

SECTION A
[25 Marks]

1. **What is the primary purpose of the General Data Protection Regulation (GDPR)?**

   A. To control government surveillance
   B. To manage company patents
   C. To protect personal data and privacy in the European Union
   D. To regulate software development practices

2. **Which of the following is considered an intellectual property in ICT?**
   A. Software code
   B. A physical computer
   C. A company's financial data
   D. Social media profiles

3. **_____is the practice of protecting computer systems, networks, and data from unauthorized access, use disclosure, disruption, modification, or destruction.**

A. cyber bullying
B. Cyber security
C. Cyber attacks
D. Protection Policies

4. **Which of the following best defines a vulnerability?**

A. A potential danger or harmful event.
B. A weakness or flaw that can be exploited.
C. The intent and capability to launch threats.
D. The likelihood of a threat occurring.

5. **What is a common form of cyberattack that encrypts a user's data and demands payment?**

A. Phishing
B. Ransomware
C. Spyware
D. Virus

6. **Which act governs cybercrimes and electronic evidence in many countries?**

A. The Computer Misuse Act
B. The Copyright Act
C. The Banking Act
D. The Securities Act

7. **What does the term "phishing" refer to in cybersecurity?**

A. Sending fake emails to trick people into providing personal information
B. Using antivirus software to protect data
C. Hacking into government websites
D. Blocking IP addresses

8. **Which of the following is a principle of data protection under GDPR?**

A. Data must be stored indefinitely
B. Data collection is mandatory for all organizations
C. Individuals cannot request their data to be deleted
D. Personal data should be processed only for the purpose it was collected

9. **What is the main objective of cybersecurity laws?**

A. To enhance user experience online
B. To safeguard electronic data and systems from unauthorized access
C. To promote new technologies
D. To restrict international communication

10. **Which of the following is NOT a security issue in ICT?**

A. Unauthorized access
B. Data encryption
C. Identity theft
D. Malware attacks

11. **What legal principle allows individuals to control how their personal information is used by organizations?**

A. Freedom of Information
B. Data Sovereignty
C. Data Protection
D. Corporate Espionage

12. **Which law protects the creation and ownership of software and algorithms?**

A. Copyright law
B. Employment law
C. Cybercrime law
D. Contract law

12. **Which type of malware can monitor and collect a user's personal data without their knowledge?**

A. Adware
B. Ransomware
C. Trojan

D. Spyware

13. **Which organization is responsible for overseeing global internet governance and cybersecurity policies?**
    A. NASA
    B. ICANN
    C. Microsoft
    D. Facebook

14. **Which of the following is an example of a denial-of-service (DoS) attack?**

    A. Unauthorized logging into a system
    B. Encrypting data with a ransomware virus
    C. Hacking into government servers
    D. Overloading a website with traffic to crash it

15. **Which legal issue arises from the unauthorized use of someone else's intellectual property?**

    A. Copyright infringement
    B. Cyberstalking
    C. Identity theft
    D. Data mining

16. **What is the role of encryption in securing data?**

    A. To organize data in storage
    B. To convert data into a secure format unreadable without a key
    C. To back up data in the cloud
    D. To delete unwanted files permanently

17. **Which of the following laws is designed to reduce email spam and protect user privacy?**

    A. CAN-SPAM Act
    B. Digital Millennium Copyright Act
    C. Child Online Protection Act
    D. Freedom of Information Act

18. **What is two-factor authentication (2FA) in cybersecurity?**

    A. A method of encrypting passwords
    B. A technique to log in using two types of credentials for added security
    C. A process of removing duplicate accounts
    D. A way of hacking into a secure system

19. **Which of the following best describes "cyberbullying"?**

A. An act of hacking into someone's account
B. Harassing or threatening someone through online communication
C. Spamming a user with email ads
D. Stealing someone's identity online

20. Which of the following best defines a firewall in network security?

A. A device that physically protects computers
B. A software that blocks unauthorized access to or from a network
C. A method for permanently deleting data
D. A tool for generating encryption keys

21. What is the primary purpose of spyware?
A. To protect the system from cyber threats.
B. To enhance the performance of the computer.
C. To monitor and gather information about a user without their consent.
D. To prevent unauthorized access to the network.

22. How does ransomware typically operate?
A. By stealing sensitive information.
B. By encrypting files and demanding a ransom for their release.
C. By spreading through email attachments.
D. By disrupting network communication.

23. Which of the following authentication types uses something the user knows?
A. Biometric authentication
B. Certificate-based authentication
C. Password authentication
D. Two-factor authentication

24. Cyber security is a significant concern for all organizations.
A. True
B. False

25. How can users protect themselves against malware infections?
A. By disabling antivirus software.
B. By downloading files from unknown sources.
C. By regularly updating software and operating systems.
D. By sharing sensitive information with unknown individuals.

SECTION B
[75 Marks]

Answer ANY THREE Questions from this Section.[25 marks each]

1. Explain following security terms.
   I. Child pornography
   II. Credit card fraud
   III. Cracking
   IV. Cyber security
   V. Identity theft

2. Explain five (5) un-ethical practices by individuals and organisations [25marks]

3. Answer the follwong 5 questions [25 Marks]
   I. What is phishing, and how can organizations protect against it?
   II. What are ethical hacking and penetration testing?
   III. What is digital forensics in the context of ICT security?
   IV. What is the role of an ICT security policy in an organization?
   V. What is identity theft, and how does it relate to ICT?

4. Explain the following cyber security terms and give at least one example [25mrks]
   I. Threats
   II. Threat Actors
   III. Computer Virus
   IV. Risk
   V. Vulnerability

5. a) Differentiate between cyber security and computer crime. [10marks]
   b) Explain the following principles. [5marks each]

   - Security awareness
   - Strong passwords
   - Data encryption