PRE BOARD EXAMINATION PAPER

FACULTY	:	**COMPUTER SCIENCE & MULTIMEDIA**
COURSE	:	**BACHELOR OF COMPUTER SCIENCE (BIT)**
		(NETWORK TECHNOLOGY & CYBER SECURITY)
YEAR / SEMESTER:		**THIRD YEAR / FIFTH SEMESTER**
MODULE TITLE	:	**CYBER SECURITY LAW & POLICY**
SUBJECT CODE	:	**CSLPA 232**
TIME ALLOWED	:	**3 HOURS**
DATE	:	**2 APRIL 2025**
SET	:	**A**

Instruction to candidates

1. This question paper has THREE (3) Sections.
2. Answer **ALL** questions in Section A, MCQ.
3. Answer **5** questions in Section B, MSAQ.
4. Answer **2** questions in Section C, MEQ.
5. No scripts or answer sheets are to be taken out of the Examination Hall.
6. For Section A, answer in the OMR form provided.

Do not open this question paper until instructed

(Candidates are required to give their answers in their own words as far as practicable)

SECTION A

Multiple Choice Questions

Attempt All Questions [30x1=30]

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

a. To allow governments to monitor all online activities

b. To ensure businesses protect consumer data

c. To regulate the use of personal data in the U.S. only

d. To limit the use of encryption technologies

2. What does the Computer Fraud and Abuse Act (CFAA) criminalize?

a. Online content piracy

b. Unauthorized access to computers and networks

c. Use of encryption software

d. Posting fake reviews online

3. Which of the following is a violation of the Electronic Communications Privacy Act (ECPA)?

a. Unauthorized access to electronic communications

b. Posting on social media

c. Downloading software updates

d. Browsing the internet in public spaces

4. There are often codes of ethics that guide the behavior of practitioners. These codes outline the expected standards and conduct within a particular profession.

a. Social Contract

b. Accountability

c. Cultural Context

d. Professional Ethics

5. Ethical behavior in cyberspace involves implementing and promoting robust security practices. This includes protecting sensitive information, using secure communication channels, and contributing to th overall cybersecurity ecosystem.

a. Privacy concerns

b. Digital Citizenship

c. Respect for Privacy

d. Security Practices

6. Core principles for processing personal information include:

a. Transparency, purpose limitation, and data minimization

b. Maximizing data collection and sharing

c. Short-term storage and immediate deletion

d. Unrestricted access for authorized personnel

7. Which international law specifically addresses cybercrimes?

a. The Geneva Convention

b. The Budapest Convention

c. The Hague Convention

d. The Paris Agreement

8. In Nepal, what is the key law regulating the protection of personal data?

a. The Cybercrime Act

b. The Electronic Transaction Act

c. The Data Protection Act

d. The Information Technology Act

9. Does focusing solely on cybersecurity laws neglect other important aspects of a safe digital future?

a. Yes, online privacy and freedom of expression matter too.

b. No, cybersecurity encompasses all online safety threats.

c. Depends on the specific context and priorities.

d. We should only focus on the most immediate threats.

10. In Nepal, which government body is responsible for addressing cybersecurity issues?

a. Nepal Police

b. National Information Technology Center (NITC)

c. Ministry of Information and Communications

d. Central Bureau of Investigation (CBI)

11. Individuals can object to processing their information:

a. Only for sensitive data

b. In any situation and for any reason

c. Based on specific, legitimate grounds

d. Never, as processing is mandatory

12. The Act protects children and vulnerable individuals:

a. Through parental consent for all processing

b. With stricter limitations on data collection and use

c. Only for specific government programs

d. Not explicitly addressed in the Act

13. What is the objective of Nepal's "National Cyber Security Strategy"?

a. To promote faster internet speeds

b. To secure critical national infrastructure and personal data

c. To support the development of cybercrime

d. To regulate e-commerce

14. Which of the following best defines "malware"?

a. A type of software that protects computers from viruses

b. A program designed to damage or disrupt a computer system

c. Software used to improve system performance

d. A tool for secure online transactions

15. Digital signatures provide which of the following?

a. Authentication

b. Non-repudiation

c. Integrity Protection

d. All of the given options are correct

16. What is the purpose of a Digital Certificate in cybersecurity?

a. To authenticate the sender's identity

b. To store sensitive data securely

c. To enhance internet speed

d. To regulate network traffic

17. Which of the following acts could be considered an example of cyber terrorism?

a. Hacking into a corporate database for financial fraud

b. Launching a large-scale DDoS attack on government websites to protest a political issue

c. Sending spam emails to millions of users

d. Stealing personal information for identity theft

18. Which of the following is an important step in mitigating the risk of cyber terrorism?

a. Regular system updates and patching vulnerabilities

b. Increasing the number of internet service providers

c. Allowing unrestricted access to critical systems

d. None of the above

19. Which of the following is a potential target for cyber terrorism attacks?

a. Government websites

b. Financial institutions

c. Power grids and critical infrastructure

d. All of the above

20. What is the role of international cooperation in combating cyber terrorism?

a. To share cyber terrorism-related data and intelligence

b. To regulate global internet access

c. To create more cyber terrorists

d. None of the above

21. Under the Electronic Transaction Act of Nepal, what is the penalty for a cyber terrorist act?

a. Imprisonment of up to 5 years

b. A fine of NPR 500,000

c. Both imprisonment and a fine

d. No penalty

22. What does "cyber intelligence" refer to?

a. Collecting and analyzing information related to cyber threats

b. Managing network traffic

c. Implementing anti-virus software

d. Encrypting sensitive data

23. Which of the following is a type of cyber attack aimed at interrupting the normal functioning of a network by overwhelming it with traffic?

a. Phishing

b. Denial of Service (DoS)

c. Malware

d. Man-in-the-Middle

24. Which type of firewall inspects data at the Application Layer?

a. Packet-filtering firewall

b. Proxy firewall

c. Stateful inspection firewall

d. Circuit-level gateway

25. Which of the following is a type of virus that spreads itself by attaching to other files or programs?

a. Worm

b. Trojan horse

c. Boot sector virus

d. File infector virus

26. Which of the following is a basic type of cyber attack that involves gaining unauthorized access to a system to steal or destroy data?

a. SQL injection

b. Eavesdropping

c. Man-in-the-Middle attack

d. Unauthorized access

27. What is the primary goal of cyber espionage?

a. To steal personal user data for financial gain

b. To gather confidential information from governments or corporations for strategic purposes

c. To encrypt files and demand ransom

d. To damage computer systems and cause financial loss

28. Which of the following is a Trojan horse virus designed to do?

a. Replicate itself and spread across networks

b. Disguise itself as legitimate software while carrying out malicious actions

c. Attach itself to executable files

d. Infect the master boot record of a computer

29. Which type of cyber-attack involves inserting malicious code into a website to steal data from users interacting with it?

a. SQL Injection

b. Cross-Site Scripting (XSS)

c. Phishing

d. Denial of Service (DoS)

30. What is the primary characteristic of a worm virus?

a. It requires a host program to spread

b. It spreads independently through networks and can replicate itself

c. It only infects mobile devices

d. It encrypts files and demands a ransom

SECTION B

Short Answer Questions

Attempt any five (5) questions out of eight (8) questions [5x6=30]

1. Define cybercrime and provide examples. [6 Marks]
2. Write short notes: (any two) [6 Marks]
   a) Cyber warfare
   b) Cyberterrorism
   c) Identity theft
3. Explain the role of international cyber policies [6 Marks]
4. What are the key components of the Nepal Cyber Policy? [6 Marks]
5. Describe why Security Governance is necessary in an organization. [6 Marks]
6. Imagine you are Chief Information Security Officer of Nepal Pharmaceutical Ltd . How do you address emerging threats like ransomware, and attacks on critical infrastructure? [6 Marks]
7. Can you provide specific examples of harmful online content that these Online Child Safety Guidelines aim to address in the Nepalese context? [6 Marks]
8. Difference between IT Governance and Security Governance. [6 Marks]

SECTION C

Long Answer Questions

Attempt any two (2) questions but question no. three (3) is compulsory. **[2x20=40]**

1. Imagine you are a cybersecurity consultant working for a Nepal Bank Limited. The organization handles sensitive customer data and wants to ensure compliance with Nepal's cybersecurity byelaws and regulatory bylaws. Now your senior management wants an Information security policy enforced on the Bank. In this regard you should prepare a Information security policy for the bank. You are tasked with researching and understanding the relevant legal framework and potential challenges. Based on that research, prepare Information Security Policy for the Bank. creating a comprehensive Information Security Policy is crucial for safeguarding the sensitive data and operations of a commercial Bank. [20 Marks]

2. Discuss the challenges and opportunities presented by cyber security laws in a global context [20 Marks]

3. **Case Study (Compulsory):** Analyze a recent incident of cybercrime and discuss the legal implications and responses. *[20 Marks]*

****** BEST OF LUCK ******

14. **Which of the following is NOT a type of cyber-attack?**

a) Denial-of-Service (DoS)
c) Man-in-the-Middle (MitM)
b) Data backup
d) SQL injection

15. **What is the main purpose of a cybersecurity policy?**

a) To punish employees
b) To establish guidelines for protecting systems and data
c) To monitor internet usage
d) To promote hacking activities

16. **Which of the following is an example of a physical security control?**

a) Firewall
c) Antivirus software
b) Security cameras
d) Encryption

17. **What is the primary purpose of a backup?**

a) To encrypt data
b) To restore data in case of loss or corruption
c) To monitor network traffic
d) To block malicious websites

18. **Which of the following is NOT a type of authentication method?**

a) Password
c) Firewall
b) Biometric
d) Two-factor authentication

19. **What is the primary purpose of a cybersecurity audit?**

a) To exploit system weaknesses
b) To assess the effectiveness of security measures
c) To launch cyberattacks
d) To monitor network traffic

20. **Which of the following is a key component of incident response?**

a) Ignoring the incident
b) Containing the incident to prevent further damage
c) Deleting all data
d) Sharing sensitive information publicly

7. **What is the primary purpose of encryption?**
   a) To delete data permanently
   b) To protect data by converting it into an unreadable format
   c) To monitor network traffic
   d) To create backups
8. **Which of the following is a key principle of GDPR?**
   a) Data minimization
   b) Unlimited data collection
   c) Sharing data without consent
   d) Ignoring data breaches
9. **What is the main purpose of a vulnerability assessment?**
   a) To exploit system weaknesses
   b) To identify and mitigate security vulnerabilities
   c) To launch cyberattacks
   d) To monitor network traffic
10. **Which of the following is NOT a type of cybercrime?**
   a) Identity theft
   b) Phishing
   c) Ethical hacking
   d) Ransomware attack
11. **What is the primary goal of ethical hacking?**
   a) To steal sensitive data
   b) To identify and fix security vulnerabilities
   c) To disrupt network services
   d) To exploit system weaknesses
12. **Which of the following is a common method of ransomware delivery?**
   a) Phishing emails
   b) Firewall configuration
   c) Data encryption
   d) Network monitoring
13. **What is the primary purpose of a VPN?**
   a) To store sensitive data
   b) To create a secure connection over the internet
   c) To monitor network traffic
   d) To encrypt physical storage devices

21. **What is the primary purpose of a honeypot?**

a) To store sensitive data

b) To attract and detect attackers

c) To encrypt data

d) To monitor network traffic

22. **Which of the following is NOT a type of cybersecurity threat?**

a) Malware

b) Phishing

c) Data backup

d) Ransomware

23. **What is the primary purpose of a cybersecurity awareness program?**

a) To punish employees

b) To educate employees about security risks and best practices

c) To monitor internet usage

d) To promote hacking activities

24. **Which of the following is an example of a cybersecurity standard?**

a) ISO 27001

b) GDPR

c) Cyber Crime Act 2018

d) Privacy Act 2018

25. **What is the primary purpose of a cybersecurity framework?**

a) To exploit system weaknesses

b) To provide guidelines for managing cybersecurity risks

c) To launch cyberattacks

d) To monitor network traffic

26. **Which of the following is NOT a type of cybersecurity control?**

a) Preventive

b) Detective

c) Destructive

d) Corrective

27. **What is the primary purpose of a cybersecurity risk assessment?**

a) To exploit system weaknesses

b) To identify and prioritize security risks

c) To launch cyberattacks

d) To monitor network traffic

28. **Which of the following is a key principle of data protection?**

a) Data minimization

b) Unlimited data collection

c) Sharing data without consent

d) Ignoring data breaches

29. **What is the primary purpose of a cybersecurity incident response plan?**

a) To ignore incidents

b) To respond to and recover from security incidents

c) To delete all data

d) To share sensitive information publicly

30. **Which of the following is NOT a type of cybersecurity attack vector?**

a) Phishing

b) Malware

c) Firewall

d) Social engineering

SECTION – B

Short Answer Questions

Attempt any five (5) questions out of eight (8) questions **[5x6=30]**

1. Define the term ransomware and explain its impact on global organizations.
2. Explain the four elements of criminal law and how they apply to cybercrime.
3. What are the key objectives of Nepal's Cybersecurity Policy? Discuss its importance in the current digital landscape.
4. Describe the stages of an Advanced Persistent Threat (APT) and the countermeasures for each stage.
5. How does ethical hacking differ from malicious hacking? Provide examples of tools used in ethical hacking.
6. Discuss the role of nation-state hackers in cyber warfare and provide examples of known attacks.
7. What is ISO 27001, and why is it important for organizations? Discuss its key components.
8. Write short notes: **(any two)**
   a. Denial-of-Service (DoS) Attack
   b. Multi-Factor Authentication (MFA)
   c. Digital Forensics

SECTION C

Long Answer Questions

Attempt any two (2) questions but question no. three (3) is compulsory. **[2x20=40]**

1. Analyze the legal and ethical implications of data breaches. Discuss the responsibilities of organizations in protecting customer data, and explain how laws like GDPR and Nepal's Cyber Crime Act 2018 address data breaches. Provide examples of high-profile data breaches and their consequences.
2. Explain the concept of Advanced Persistent Threats (APTs) and their impact on organizations. Discuss the stages of an APT attack, and provide detailed countermeasures that organizations can implement to defend against such threats.
3. Explain the concept of vulnerability assessment in cybersecurity. Describe the methodologies used and provid examples of tools for conducting vulnerability assessments. explain the importance of incident response plannin in cybersecurity. Outline the key steps in developing an incident response plan.

Best of Luck