

JK

Roll No. _____

Question Booklet Number

O.M.R. Serial No. :

--	--	--	--	--	--	--	--

--

BCA VI Semester (NEP Back) Examination, 2025-26

Information and Cyber Security

Paper Code						
B	C	A	6	0	0	1

Question Booklet Series

A

Time : 1 : 30 Hours]

[Maximum Marks : 75

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 100 questions. Examinee is required to answer 75 questions in the OMR Answer-Sheet provided and not in the question booklet. **All** questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.
4. Four alternative answers are mentioned for each question as – A, B, C & D in the booklet. The candidate has to choose the correct answer and mark the same in the OMR Answer-Sheet as per the direction :

(Remaining instructions on the last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को 75 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। **सभी** प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गये हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, तो उसे तुरन्त बदल लें।
4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर- A, B, C तथा D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छँटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

Rough Work

रफ़ कार्य

1. What is cyberspace?
 - (A) Physical cables
 - (B) Virtual internet environment
 - (C) Hardware
 - (D) Hacker
2. Netizens are:
 - (A) Hackers
 - (B) Neutral mind people
 - (C) Developers
 - (D) Internet users
3. IT Act implemented in:
 - (A) 1995
 - (B) 1998
 - (C) 2000
 - (D) 2005
4. Objective of IT Act is:
 - (A) Hardware control
 - (B) Legal recognition of e-records
 - (C) Programming
 - (D) Networking
5. Electronic records are:
 - (A) Paper files
 - (B) Digital data
 - (C) Verbal data
 - (D) Books
6. IDS stands for:
 - (A) Internal Delivery System
 - (B) Intrusion Detection System
 - (C) Internet Data Service
 - (D) Input Data System
7. IPS stands for:
 - (A) Internet Protection System
 - (B) Input Processing System
 - (C) Intrusion Prevention System
 - (D) Internal Protection System
8. IDS is used to:
 - (A) Prevent attacks
 - (B) Detect intrusions
 - (C) Store data
 - (D) Encrypt data

9. IPS is used to:
- (A) Monitor only
 - (B) Detect and prevent attacks
 - (C) Backup data
 - (D) Speed network
10. Scope of IT Act includes:
- (A) Cybercrime and e-governance
 - (B) firewall
 - (C) Printing
 - (D) Storage
11. Cyber jurisdiction means:
- (A) Hardware control
 - (B) Legal authority in cyberspace
 - (C) Programming
 - (D) Networking
12. PKI stands for:
- (A) Public Key Internet
 - (B) Private Key Infrastructure
 - (C) Protected Key Interface
 - (D) Public Knowledge Index
13. Digital certificates are issued by:
- (A) Users
 - (B) CCA
 - (C) Certifying Authorities
 - (D) ISPs
14. Encryption means:
- (A) Deleting data
 - (B) Copying data
 - (C) Making data unrecognizable
 - (D) Compressing data
15. Anomaly-based IDS detects:
- (A) Known attacks
 - (B) Software bugs
 - (C) deviations from normal behaviour
 - (D) Hardware faults
16. Cyber ethics refers to:
- (A) Hardware design
 - (B) Moral rules in cyberspace
 - (C) Networking
 - (D) Coding

17. IT Act provides legal status to:

- (A) Paper records
- (B) Cryptography
- (C) Electronic transactions
- (D) Printers

18. Certifying Authority issues:

- (A) Passwords
- (B) Digital certificates
- (C) Firewalls
- (D) Antivirus

19. Cyber law deals with:

- (A) Physical crimes
- (B) Cyber crimes
- (C) Traffic rules
- (D) Banking only

20. PKI includes:

- (A) Router
- (B) Digital certificate
- (C) Switch
- (D) Cable

21. What is computer security?

- (A) Protecting hardware
- (B) Adding threat
- (C) Programming
- (D) Protecting systems from threats

22. Which of the following is a cyber threat?

- (A) Printer
- (B) Virus
- (C) Mouse
- (D) Keyboard

23. Hacking refers to:

- (A) Unauthorized access
- (B) Securing systems
- (C) Data storage
- (D) Programming

24. Cracking means:

- (A) Ethical hacking
- (B) Breaking security systems
- (C) Coding
- (D) Testing software

25. Sneaking refers to:

- (A) Authorized access
- (B) Software hacking
- (C) Hidden unauthorized access
- (D) Debugging

26. A computer virus is:

- (A) Hardware
- (B) Malware
- (C) Antivirus
- (D) Firewall

27. Trojan Horse is:

- (A) Antivirus
- (B) Malware disguised as legitimate software
- (C) Firewall
- (D) Router

28. Worms are:

- (A) Hardware bugs
- (B) Type of virus
- (C) Firewalls
- (D) Self-replicating malware

29. Malicious code includes:

- (A) Software bugs
- (B) Harmful programs
- (C) Drivers
- (D) OS

30. Logic bomb activates:

- (A) Immediately
- (B) Randomly
- (C) Based on specific condition
- (D) Never

31. DoS attack aims to:

- (A) Attack on confidentiality
- (B) To attack on availability
- (C) Attack on authentication
- (D) Backup data

32. Phishing is:

- (A) Fishing activity
- (B) Fake communication to steal data
- (C) Antivirus
- (D) Firewall

33. MITM attack means:

- (A) System crash
- (B) Meet in the middle
- (C) Intercepting communication
- (D) Programming

34. Script kiddies are:
- (A) Expert hackers
 - (B) Inexperienced attackers using tools
 - (C) Developers
 - (D) Admins
35. Firewall is used for:
- (A) Storage
 - (B) Network security
 - (C) Programming
 - (D) Gaming
36. Social engineering involves:
- (A) Manipulating people
 - (B) Torturing people
 - (C) Coding
 - (D) Networking
37. Password attack targets:
- (A) Hardware
 - (B) User credentials
 - (C) Network cables
 - (D) Printers
38. Ransomware does:
- (A) Protect data
 - (B) Backup data
 - (C) Locks data for ransom
 - (D) Delete OS
39. Network attack means:
- (A) Physical damage
 - (B) Unauthorized network access
 - (C) Software update
 - (D) Programming
40. Defense against attacks includes:
- (A) Ignoring threats
 - (B) Using security tools
 - (C) Sharing passwords
 - (D) Disabling firewall
41. Wireless networks use:
- (A) Cables
 - (B) Radio waves
 - (C) Fiber only
 - (D) Satellites only

42. Bluetooth is used for:
- (A) Short distance networking
 - (B) Long-range communication
 - (C) Storage
 - (D) Processing
43. WEP is:
- (A) Strong security
 - (B) Weak encryption protocol
 - (C) Firewall
 - (D) Antivirus
44. WPA2 uses:
- (A) No encryption
 - (B) Strong encryption
 - (C) Only passwords
 - (D) Open network
45. Rogue access point is:
- (A) Authorized AP
 - (B) Unauthorized AP
 - (C) Router
 - (D) Switch
46. Wi-Fi sniffing is:
- (A) Data encryption
 - (B) Capturing network traffic
 - (C) Blocking network
 - (D) Repairing network
47. MAC filtering works on:
- (A) IP address
 - (B) MAC address
 - (C) URL
 - (D) Password
48. Mobile security protects:
- (A) Only calls
 - (B) Smartphones and data
 - (C) Hardware only
 - (D) Network cables
49. SIM cloning means:
- (A) SIM repair
 - (B) Copying SIM data
 - (C) Blocking SIM
 - (D) Destroying SIM
50. BYOD stands for:
- (A) Bring Your Own Device
 - (B) Build Your Own Data
 - (C) Backup Your Own Data
 - (D) Buy Your Own Device

51. Two-factor authentication requires:
- (A) One password
 - (B) Two verification steps
 - (C) No password
 - (D) Only OTP
52. Wireless encryption protects:
- (A) Hardware
 - (B) Data transmission
 - (C) Power supply
 - (D) Speed
53. Common wireless attack is:
- (A) Phishing
 - (B) Eavesdropping
 - (C) Printing
 - (D) Backup
54. Smartphone pentesting is:
- (A) Repairing phone
 - (B) Testing mobile security
 - (C) Charging phone
 - (D) Updating apps
55. Mobile app security focuses on:
- (A) Hardware
 - (B) Application vulnerabilities
 - (C) Battery
 - (D) Screen
56. Hotspot security risk includes:
- (A) Strong encryption
 - (B) Open access
 - (C) Firewall
 - (D) VPN
57. Wireless network is vulnerable due to:
- (A) Physical wires
 - (B) Open signals
 - (C) Hardware
 - (D) CPU
58. Encryption method in Wi-Fi:
- (A) AES
 - (B) DES
 - (C) HTTP
 - (D) FTP

59. Network authentication ensures:
- (A) Speed
 - (B) Identity verification
 - (C) Storage
 - (D) Backup
60. Securing Wi-Fi includes:
- (A) Open access
 - (B) Strong passwords
 - (C) No password
 - (D) Public sharing
61. ISO 27001 relates to:
- (A) Networking
 - (B) Information security management
 - (C) Hardware
 - (D) Software
62. ISMS stands for:
- (A) Information Security Management System
 - (B) Internet System
 - (C) Internal Security Model
 - (D) Integrated Software Model
63. Cyber law deals with:
- (A) Physical crimes
 - (B) Digital crimes
 - (C) Traffic laws
 - (D) Banking only
64. IT Act 2000 applies to:
- (A) Only hardware
 - (B) Electronic transactions
 - (C) Only banks
 - (D) Only emails
65. Security audit is:
- (A) Hacking
 - (B) Network evaluation
 - (C) Programming
 - (D) Evaluation of security
66. Cybercrime investigation involves:
- (A) Coding
 - (B) Evidence collection
 - (C) Hardware design
 - (D) Testing

67. Digital evidence is:

- (A) Paper
- (B) Electronic form
- (C) Verbal proof
- (D) Books

68. CERT-In is:

- (A) Company
- (B) Cyber security organization
- (C) Software
- (D) Hardware

69. Compliance means:

- (A) Ignoring rules
- (B) Following standards
- (C) Breaking laws
- (D) Coding

70. Risk assessment identifies:

- (A) Data
- (B) Threats
- (C) Hardware
- (D) Programs

71. Security standards ensure:

- (A) Speed
- (B) Safety
- (C) Storage
- (D) Coding

72. Information Security policy revolved around :

- (A) ABC triad
- (B) External
- (C) CIA triad
- (D) BIA triad

73. Cyber tribunal handles:

- (A) Physical crimes
- (B) Cyber disputes
- (C) Traffic
- (D) Banking

74. Investigation agency collects:

- (A) Hardware
- (B) Evidence
- (C) Software
- (D) Data cables

75. Data protection laws ensure:

- (A) Data misuse
- (B) Encryption
- (C) Confidentiality
- (D) Deletion

76. Audit report provides:
- (A) Threats
 - (B) Findings
 - (C) Errors
 - (D) Data
77. Legal framework ensures:
- (A) Proper Regulation
 - (B) Chaos
 - (C) Errors
 - (D) Hacking
78. IT Act covers:
- (A) Only emails
 - (B) E-commerce
 - (C) Only banking
 - (D) Only hardware
79. Forensics supports:
- (A) Crime investigation
 - (B) Coding
 - (C) Networking
 - (D) Hardware
80. Cyber standards improve:
- (A) Risk
 - (B) Security
 - (C) Errors
 - (D) Attacks
81. Disaster recovery means:
- (A) Data loss
 - (B) Restoring systems
 - (C) Deleting data
 - (D) Ignoring issues
82. DRP stands for:
- (A) Disaster Recovery Plan
 - (B) Device Recovery Plan
 - (C) Digital Risk Plan
 - (D) Data Risk Process
83. Digital signature ensures:
- (A) Speed
 - (B) Authenticity
 - (C) Storage
 - (D) Deletion

84. Penetration testing is:
- (A) Attacking system
 - (B) Testing accuracy
 - (C) Deleting data
 - (D) Testing loophole in system
85. Vulnerability assessment finds:
- (A) Strength
 - (B) Weakness
 - (C) Speed
 - (D) Storage
86. Computer forensics deals with:
- (A) Hardware
 - (B) Digital evidence
 - (C) Networking
 - (D) Programming
87. Forensics investigation helps in :
- (A) Data deletion
 - (B) Coding
 - (C) Chain of custody
 - (D) Testing
88. Chain of custody ensures:
- (A) Data loss
 - (B) Evidence integrity
 - (C) Speed
 - (D) Storage
89. Incident response handles:
- (A) Normal operation
 - (B) Security incidents
 - (C) Hardware
 - (D) Software
90. Risk management reduces:
- (A) Security
 - (B) Encryption
 - (C) Threat
 - (D) Speed
91. Backup strategy protects:
- (A) Hardware
 - (B) Data
 - (C) Network cables
 - (D) CPU

92. Data recovery restores:
- (A) Lost data
 - (B) Hardware
 - (C) Programs
 - (D) OS
93. Forensic tools are used for:
- (A) Gaming
 - (B) Investigation
 - (C) Coding
 - (D) Networking
94. Log analysis helps in:
- (A) Ignoring data
 - (B) Merging issues
 - (C) Deleting logs
 - (D) Better issue finding
95. Ethical hackers are:
- (A) Criminals
 - (B) Security professionals
 - (C) Users
 - (D) Students
96. Pen testing simulates:
- (A) Normal use
 - (B) Loophole
 - (C) Attacks
 - (D) Backup
97. Digital evidence must be:
- (A) Modified
 - (B) Preserved
 - (C) Deleted
 - (D) Ignored
98. Disaster recovery focuses on:
- (A) Normalcy Restoration
 - (B) ISMS
 - (C) Hacking
 - (D) Coding
99. Security management ensures:
- (A) Risk
 - (B) Protection
 - (C) Loss
 - (D) Errors
100. Digital Signature is important for:
- (A) Confidentiality
 - (B) Coding
 - (C) Hardware
 - (D) Authentication

Rough Work
रफ़ कार्य

Example :

Question :

- Q. 1 (A) (B) (C) (D)
- Q. 2 (A) (B) (C) (D)
- Q. 3 (A) (B) (C) (D)

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.
6. All answers are to be given on OMR Answer Sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.
7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.
8. After the completion of the examination candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.
9. There will be no negative marking.
10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.
11. To bring and use of log-book, calculator, pager & cellular phone in examination hall is prohibited.
12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is any discrepancy in the question booklet, then after showing it to the invigilator, get another question booklet of the same series.

उदाहरण :

प्रश्न :

- प्रश्न 1 (A) (B) (C) (D)
- प्रश्न 2 (A) (B) (C) (D)
- प्रश्न 3 (A) (B) (C) (D)

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।
6. सभी उत्तर केवल ओ.एम.आर. उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।
7. ओ.एम.आर. उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।
8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।
9. निगेटिव मार्किंग नहीं है।
10. कोई भी रफ कार्य, प्रश्न-पुस्तिका में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।
11. परीक्षा कक्ष में लॉग-बुक, कैल्कुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।
12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्ण : प्रश्न-पुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्न-पुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्न-पुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सीरीज की दूसरी प्रश्न-पुस्तिका प्राप्त कर लें।