Roll. No. ....

O.M.R. Serial No. | | | | | | | |

Question Booklet Number

B.A. (FYUP) (SEM.-II) EXAMINATION, 2025-26
VOCATIONAL COURSE
CYBER SECURITY
[CODE : VOC-160]

Paper Code							
A	9	0	1	0	1	5	T

Question Booklet Series
D

Time : 1 : 00 Hours **Max. Marks : 60**

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 60 questions. Examinee is required to answer all 60 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 last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 60 प्रश्न हैं। परीक्षार्थी को सभी 60 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 गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, उसे तुरन्त बदल लें।
4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर- A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

1. Why is it important to involve parents, teachers, and guardians in digital safety efforts ?

(A) They can provide guidance, set boundaries, and monitor harmful behavior

(B) They can restrict internet completely

(C) They stop all online fun

(D) They can create viral videos

2. What is the most common tool used to access the dark web ?

(A) TOR (The Onion Router) browser

(B) WhatsApp

(C) Google Chrome

(D) Safari

3. Which of the following is an effective preventive measure against cyber terrorism ?

(A) Ignoring updates

(B) Clicking unknown ads

(C) Regularly updating software and practicing digital hygiene

(D) Using outdated antivirus

1. डिजिटल सुरक्षा की कोशिशों में माता-पिता, शिक्षकों और अभिभावकों को शामिल करना क्यों जरूरी है ?

(A) वे गाइडेंस दे सकते हैं, सीमाएं तय कर सकते हैं और नुकसानदायक व्यवहार पर नज़र रख सकते हैं

(B) वे इंटरनेट को पूरी तरह से बैन कर सकते हैं

(C) वे ऑनलाइन सारा मज़ा रोक देते हैं

(D) वे वायरल वीडियों बना सकते हैं

2. डार्क वेब एक्सेस करने के लिए सबसे आम टूल कौन-सा है ?

(A) TOR (द अनियन राउटर) ब्राउज़र

(B) वाट्सएप

(C) गुगल क्रोम

(D) सफारी

3. निम्नलिखित में से कौन-सा साइबर आतंकवाद के खिलाफ एक असरदार बचाव का तरीका है ?

(A) अपडेट्स को नजरअंदाज़ करना

(B) अनजान विज्ञापनों पर क्लिक करना

(C) सॉफ्टवेयर को रेगुलर अपडेट करना और डिजिटल हाइजीन का पालन करना

(D) पुराने एंटीवायरस का इस्तेमाल करना

4. Virus is :
   - (A) Hardware
   - (B) Malware
   - (C) Protocol
   - (D) Network

4. वायरस है :
   - (A) हार्डवेयर
   - (B) मैलवेयर
   - (C) प्रोटोकॉल
   - (D) नेटवर्क

5. Worm spreads :
   - (A) Manually
   - (B) Automatically
   - (C) Offline
   - (D) Slowly

5. वर्म फैलता है :
   - (A) मैन्युअली
   - (B) ऑटोमैटिकली
   - (C) ऑफ़लाइन
   - (D) धीरे-धीरे

6. Trojan horse is :
   - (A) Safe software
   - (B) Network
   - (C) Firewall
   - (D) Hidden malware

6. ट्रोजन हॉर्स है :
   - (A) सुरक्षित सॉफ्टवेयर
   - (B) नेटवर्क
   - (C) फ़ायरवॉल
   - (D) छिपा हुआ मैलवेयर

7. Spyware is used to :
   - (A) Protect data
   - (B) Monitor user activity
   - (C) Delete files
   - (D) Encrypt data

7. स्पाइवेयर का उपयोग किया जाता है :
   - (A) डेटा की सुरक्षा के लिए
   - (B) उपयोगकर्ता की गतिविधि पर नज़र रखने के लिए
   - (C) फ़ाइलों को हटाने के लिए
   - (D) डेटा को एन्क्रिप्ट करने के लिए

8. Antivirus is used to :
   - (A) Attack system
   - (B) Slow system
   - (C) Delete OS
   - (D) Detect malware

8. एंटीवायरस का उपयोग किया जाता है :
   - (A) सिस्टम पर हमला करने के लिए
   - (B) सिस्टम को धीमा करने के लिए
   - (C) OS को डिलीट करने के लिए
   - (D) मैलवेयर का पता लगाने के लिए

9. Identity theft means :

(A) Stealing identity

(B) Deleting files

(C) Hacking server

(D) Coding

10. Cybercrime includes :

(A) Hacking

(B) Phishing

(C) Fraud

(D) All of the above

11. Which sector needs cybersecurity most ?

(A) Banking

(B) Healthcare

(C) Education

(D) All of the above

12. Two-factor authentication uses :

(A) One step

(B) Two methods

(C) No password

(D) Only OTP

13. Biometric authentication includes :

(A) Password

(B) Fingerprint

(C) Username

(D) Email

9. पहचान की चोरी का अर्थ है :

(A) पहचान चुराना

(B) फ़ाइल मिटाना

(C) सर्वर हैक करना

(D) कोडिंग

10. साइबर अपराध में शामिल हैं :

(A) हैकिंग

(B) फ़िशिंग

(C) धोखाधड़ी

(D) उपरोक्त सभी

11. किस क्षेत्र को साइबर सुरक्षा की सबसे अधिक आवश्यकता है ?

(A) बैंकिंग

(B) स्वास्थ्य सेवा

(C) शिक्षा

(D) उपरोक्त सभी

12. टू-फैक्टर ऑथेंटिकेशन में उपयोग होता है :

(A) एक चरण

(B) दो तरीके

(C) कोई पासवर्ड नहीं

(D) केवल OTP

13. बायोमेट्रिक प्रमाणीकरण में शामिल है :

(A) पासवर्ड

(B) फिंगरप्रिंट

(C) यूज़रनेम

(D) ईमेल

14. A threat is :

(A) Protection mechanism

(B) Potential harm

(C) Security tool

(D) Software

15. Vulnerability is :

(A) Strength

(B) Weakness in system

(C) Attack

(D) Tool

16. Risk is :

(A) Threat × Vulnerability

(B) Data × Security

(C) Software × Hardware

(D) None of these

17. Which is an example of threat ?

(A) Firewall

(B) Hacker

(C) Antivirus

(D) Encryption

18. Which is a vulnerability ?

(A) Weak password

(B) Antivirus

(C) Backup

(D) Firewall

14. खतरा है :

(A) सुरक्षा तंत्र

(B) संभावित नुकसान

(C) सुरक्षा उपकरण

(D) सॉफ्टवेयर

15. भेद्यता है :

(A) शक्ति

(B) तन्त्र में कमजोरी

(C) हमला

(D) उपकरण

16. जोखिम है :

(A) खतरा × भेद्यता

(B) डेटा × सुरक्षा

(C) सॉफ्टवेयर × हार्डवेयर

(D) इनमें से कोई नहीं

17. खतरे का एक उदाहरण कौन-सा है ?

(A) फ़ायरवॉल

(B) हैकर

(C) एंटीवायरस

(D) एन्क्रिप्शन

18. इनमें से कौन-सी एक कमज़ोरी (vulnerability) है ?

(A) कमज़ोर पासवर्ड

(B) एंटीवायरस

(C) बैकअप

(D) फ़ायरवॉल

19. To stay safe, users should scan :

(A) QR codes from random walls

(B) Only QR codes from trusted sources

(C) Any QR during emergencies

(D) Faded QR codes

20. What is the key legal body in India that provides technical help in cyber attacks and phishing ?

(A) RBI

(B) MeitY

(C) CERT-IN

(D) UIDAI

21. Who can complain to the RBI Ombudsman ?

(A) Only businessmen

(B) Anyone having a banking issue

(C) Only NRIs

(D) Only RBI staff

22. Which of these actions is a safe response to cyberbullying ?

(A) Create a fake account to fight back

(B) Block and report the bully on the platform

(C) Keep it a secret

(D) Share bullying post with others

19. सुरक्षित रहने के लिए, यूज़र्स को स्कैन करना चाहिए :

(A) रैंडम दीवारों पर लगे QR कोड

(B) सिर्फ़ भरोसेमंद सोर्स से मिले QR कोड

(C) इमरजेंसी के दौरान कोई भी QR कोड

(D) हल्के पड़े QR कोड

20. भारत में वह मुख्य कानूनी संस्था कौन-सी है जो साइबर हमलों और फ़िशिंग में तकनीकी मदद देती है ?

(A) RBI

(B) MeitY

(C) CERT-IN

(D) UIDAI

21. RBI ओम्बुड्समैन से कौन शिकायत कर सकता है ?

(A) सिर्फ बिजनेसमैन

(B) बैंकिंग समस्या वाला कोई भी व्यक्ति

(C) सिर्फ NRI

(D) सिर्फ RBI स्टाफ

22. इनमें से कौन-सा काम साइबरबुलिंग का सुरक्षित जवाब है ?

(A) जवाब देने के लिए एक फ़ेक अकाउंट बनाना

(B) प्लेटफ़ार्म पर बुली को ब्लॉक और रिपोर्ट करना

(C) इसे सीक्रेट रखना

(D) बुलिंग पोस्ट दूसरों के साथ शेयर करना

23. Digital signature ensures :

(A) Speed

(B) Authenticity

(C) Storage

(D) Format

24. Risk management includes :

(A) Ignoring threats

(B) Identifying threats

(C) Deleting files

(D) Formatting

25. Security policy is :

(A) Rules for protection

(B) Software

(C) Hardware

(D) Network

26. Cybersecurity protects against :

(A) Theft

(B) Damage

(C) Unauthorized access

(D) All of these

27. Ethical hacking is :

(A) Illegal

(B) Legal testing

(C) Criminal activity

(D) Fraud

23. डिजिटल हस्ताक्षर सुनिश्चित करता है :

(A) गति

(B) प्रामाणीकता

(C) भंडारण

(D) प्रारूप

24. जोखिम प्रबन्धन में शामिल होता है :

(A) खतरों को नजरअंदाज करना

(B) खतरों को पहचानना

(C) फाइलो को डिलीट करना

(D) फार्मेटिंग

25. सुरक्षा नीति है :

(A) सुरक्षा के नियम

(B) सॉफ्टवेयर

(C) हार्डवेयर

(D) नेटवर्क

26. साइबर सिक्योरिटी इनसे बचाती है :

(A) चोरी

(B) नुकसान

(C) बिना इजाज़त के एक्सेस

(D) इनमे से सभी

27. एथिकल हैकिंग है :

(A) अवैध

(B) कानूनी परीक्षण

(C) आपराधिक गतिविधि

(D) धोखाधड़ी

28. Information security focuses on :

(A) Protecting information

(B) Coding

(C) Gaming

(D) Hardware only

29. First step in security is :

(A) Prevention

(B) Awareness

(C) Recovery

(D) Attack

30. Trusted contacts in account recovery are :

(A) Random people online

(B) Friends chosen by you to help recover your account

(C) Police officers

(D) Tech support agents

31. Reviewing recent login history helps you to :

(A) Learn time management

(B) Check if someone logged in from unknown devices

(C) Increase followers

(D) Find new friends

32. A dangerous QR code often :

(A) Opens unknown suspicious links

(B) Shows a wallpaper

(C) Opens camera

(D) Plays music

28. सूचना सुरक्षा किस पर केंद्रित है ?

(A) सूचना की सुरक्षा पर

(B) कोडिंग पर

(C) गेमिंग पर

(D) केवल हार्डवेयर पर

29. सुरक्षा का पहला कदम है :

(A) रोकथाम

(B) जागरूकता

(C) रिकवरी

(D) हमला

30. अकाउंट रिकवरी में भरोसेमंद कॉन्टैक्ट्स होते हैं :

(A) ऑनलाइन अनजान लोग

(B) आपके द्वारा चुने गए दोस्त जो आपका अकाउंट रिकवर करने में मदद करते हैं

(C) पुलिस अधिकारी

(D) टेक सपोर्ट एजेंट

31. हाल की लॉगिन हिस्ट्री देखने से आपको मदद मिलती है :

(A) टाइम मैनेजमेंट सीखने में

(B) यह चेक करने में कि क्या किसी ने अनजान डिवाइस से लॉग इन किया है

(C) फॉलोअर्स बढ़ाने में

(D) नए दोस्त ढूँढ़ने में

32. एक खतरनाक QR कोड अक्सर :

(A) अनजान संदिग्ध लिंक खोलता है

(B) वॉलपेपर दिखाता है

(C) कैमरा खोलता है

(D) म्यूजिक बजाता है

33. Cybersecurity refers to :

(A) Protecting hardware only

(B) Protecting data, systems, and networks

(C) Developing applications

(D) Internet usage

34. Which of the following is a cyber asset ?

(A) Data

(B) Hardware

(C) Software

(D) All of the above

35. Which goal ensures data is not disclosed to unauthorized users ?

(A) Integrity

(B) Availability

(C) Confidentiality

(D) Authentication

36. Integrity ensures :

(A) Data is always available

(B) Data is accurate and unchanged

(C) Data is hidden

(D) Data is deleted

37. Availability means :

(A) Data is always secure

(B) Data is accessible when needed

(C) Data is encrypted

(D) Data is hidden

33. साइबर सुरक्षा का तात्पर्य है :

(A) केवल हार्डवेयर की सुरक्षा करना

(B) डेटा, सिस्टम और नेटवर्क की सुरक्षा करना

(C) एप्लिकेशन विकसित करना

(D) इंटरनेट का उपयोग

34. निम्नलिखित में से कौन-सी एक साइबर संपत्ति है ?

(A) डेटा

(B) हार्डवेयर

(C) सॉफ्टवेयर

(D) उपरोक्त सभी

35. कौन-सा लक्ष्य यह सुनिश्चित करता है कि डेटा अनधिकृत उपयोगकर्ताओं को प्रकट न हो ?

(A) अखंडता

(B) उपलब्धता

(C) गोपनीयता

(D) प्रमाणीकरण

36. अखंडता यह सुनिश्चित करती है कि :

(A) डेटा हमेशा उपलब्ध रहे

(B) डेटा सटीक और अपरिवर्तित रहे

(C) डेटा छिपा रहे

(D) डेटा हटा दिया जाए

37. उपलब्धता का अर्थ है :

(A) डेटा हमेशा सुरक्षित रहता है

(B) ज़रूरत पड़ने पर डेटा उपलब्ध होता है

(C) डेटा एन्क्रिप्टेड होता है

(D) डेटा छिपा हुआ होता है

38. White hat hackers are :
(A) Criminals
(B) Ethical hackers
(C) Beginners
(D) Employees

39. Black hat hackers :
(A) Protect systems
(B) Hack maliciously
(C) Test systems
(D) Secure networks

40. Grey hat hackers :
(A) Always legal
(B) Mix of ethical and unethical
(C) Only criminals
(D) Beginners

41. Script kiddies are :
(A) Experts
(B) Use ready-made tools
(C) Developers
(D) Engineers

42. Hacktivists are motivated by :
(A) Money
(B) Learning
(C) Politics or ideology
(D) Fun

43. Malware stands for :
(A) Malicious software
(B) Managed software
(C) Manual software
(D) Machine software

38. व्हाइट हैट हैकर्स होते हैं :
(A) अपराधी
(B) एथिकल हैकर्स
(C) शुरूआती लोग
(D) कर्मचारी

39. ब्लैक हैट हैकर्स :
(A) सिस्टम्स की सुरक्षा करते हैं
(B) दुर्भावनापूर्ण तरीके से हैक करते हैं
(C) सिस्टम्स का परीक्षण करते हैं
(D) नेटवर्क्स को सुरक्षित करते हैं

40. ग्रे हैट हैकर्स होते है :
(A) हमेशा कनूनी
(B) नैतिक और अनैतिक का मिश्रण
(C) केवल अपराधी
(D) शुरूआती

41. स्क्रिप्ट किडीज़ होते हैं :
(A) विशेषज्ञ
(B) बने-बनाए टूल्स का उपयोग करते हैं
(C) डेवलपर्स
(D) इंजीनियर

42. हैकटिविस्ट्स को किससे प्रेरणा मिलती है ?
(A) पैसा
(B) सीखना
(C) राजनीति या विचारधारा
(D) मज़ा

43. Malware का अर्थ है :
(A) दुर्भाग्यपूर्ण सॉफ्टवेयर
(B) प्रबंधित सॉफ्टवेयर
(C) मैनुअल सॉफ्टवेयर
(D) मशीन सॉफ्टवेयर

44. Firewall is used for :

(A) Data storage

(B) Network protection

(C) Coding

(D) Gaming

45. Backup helps in :

(A) Preventing attacks

(B) Encrypting files

(C) Speeding system

(D) Recovering data

46. Encryption provides :

(A) Speed

(B) Security

(C) Storage

(D) Deletion

47. Password should be :

(A) Simple

(B) Short

(C) Complex

(D) Same everywhere

48. Cybersecurity is important for :

(A) Businesses

(B) Individuals

(C) Government

(D) All of the above

49. Data breach leads to :

(A) Profit

(B) Data loss

(C) Speed

(D) Storage

44. फ़ायरवॉल का उपयोग किया जाता है :

(A) डेटा स्टोरेज के लिए

(B) नेटवर्क सुरक्षा के लिए

(C) कोडिंग के लिए

(D) गेमिंग के लिए

45. बैकअप इसमें मदद करता है :

(A) हमलों को रोकने में

(B) फ़ाइलों को एन्क्रिप्ट करने में

(C) सिस्टम की गति बढ़ाने में

(D) डेटा रिकवर करने में

46. एन्क्रिप्शन प्रदान करता है :

(A) गति

(B) सुरक्षा

(C) भंडारण

(D) विलोपन

47. पासवर्ड होना चाहिए :

(A) सरल

(B) छोटा

(C) जटिल

(D) हर जगह एक जैसा

48. साइबर सुरक्षा किसके लिए महत्वपूर्ण है ?

(A) व्यवसायों के लिए

(B) व्यक्तियों के लिए

(C) सरकार के लिए

(D) उपरोक्त सभी के लिए

49. डेटा ब्रीच से होता है :

(A) लाभ

(B) डेटा की हानि

(C) गति

(D) स्टोरेज

50. CIA triad includes :

(A) Confidentiality, Integrity, Availability

(B) Control, Internet, Access

(C) Code, Interface, Application

(D) None of these

51. Authentication verifies :

(A) Data accuracy

(B) User identity

(C) Network speed

(D) File size

52. Authorization determines :

(A) Who are you

(B) What you can access

(C) How data is stored

(D) How fast system works

53. Non-repudiation ensures :

(A) Data deletion

(B) Sender cannot deny action

(C) Fast access

(D) Encryption

54. Which is NOT a security service ?

(A) Authentication

(B) Authorization

(C) Compression

(D) Confidentiality

50. CIA ट्रायड में शामिल हैं :

(A) गोपनीयता, अखंडता, उपलब्धता

(B) नियंत्रण, इंटरनेट, पहुँच

(C) कोड, इंटरफ़ेस, एप्लिकेशन

(D) इनमें से कोई नहीं

51. प्रमाणीकरण इसकी पुष्टि करता है :

(A) डेटा की सटीकता

(B) उपयोगकर्ता की पहचान

(C) नेटवर्क की गति

(D) फ़ाइल का आकार

52. ऑथराइज़ेशन यह निर्धारित करता है :

(A) आप कौन हैं

(B) आप किस चीज़ तक पहुँच सकते हैं

(C) डेटा कैसे स्टोर किया जाता है

(D) सिस्टम कितनी तेज़ी से काम करता है

53. नॉन-रेप्यूडिएशन यह सुनिश्चित करता है :

(A) डेटा हटाना

(B) भेजने वाला अपने कार्य से इन्कार नहीं कर सकता

(C) तेज पहुँच

(D) एन्क्रिप्शन

54. इनमें से कौन-सी एक सुरक्षा सेवा नहीं है ?

(A) प्रमाणीकरण

(B) प्राधिकरण

(C) संपीड़न

(D) गापनीयता

55. Patch management is used to :

(A) Fix vulnerabilities

(B) Delete files

(C) Increase size

(D) Format disk

56. Zero-day attack targets :

(A) Known vulnerabilities

(B) Unknown vulnerabilities

(C) Hardware

(D) Network cables

57. Insider threat comes from :

(A) External hacker

(B) Internal user

(C) Antivirus

(D) Firewall

58. Cyber hygiene refers to :

(A) Cleaning computer

(B) Safe practices

(C) Formatting system

(D) Deleting data

59. Strong security reduces :

(A) Risk

(B) Storage

(C) Speed

(D) Access

60. Cyber attack targe t:

(A) Data

(B) Systems

(C) Networks

(D) All of these

55. पैच मैनेज़मेंट का उपयोग किया जाता है :

(A) कमज़ोरियों को ठीक करने के लिए

(B) फ़ाइलों को हटाने के लिए

(C) आकार बढ़ाने के लिए

(D) डिस्क को फ़ॉर्मेट करने के लिए

56. Zero-day attack के लक्ष्य हैं :

(A) ज्ञात कमज़ोरियाँ

(B) अज्ञात कमज़ोरियाँ

(C) हार्डवेयर

(D) नेटवर्क केबल

57. इनसाइडर थ्रेट आता है :

(A) बाहरी हैकर से

(B) आंतरिक उपयोगकर्ता से

(C) एंटीवायरस से

(D) फ़ायरवॉल से

58. साइबर हाइजीन का अर्थ है :

(A) कम्प्यूटर की सफाई

(B) सुरक्षित अभ्यास

(C) सिस्टम को फॉर्मेट करना

(D) डेटा को हटाना

59. कम्प्यूटर सुरक्षा कम करती है :

(A) जोखिम

(B) स्टोरेज

(C) गति

(D) पहुँच

60. साइबर हमले का निशाना होता है :

(A) डेटा

(B) सिस्टम

(C) नेटवर्क

(D) इनमें से सभी

Rough Work / रफ कार्य

Example :

Question :

Q.1 Ⓐ ● Ⓒ Ⓓ

Q.2 Ⓐ Ⓑ ● Ⓓ

Q.3 Ⓐ ● Ⓒ Ⓓ

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 Ⓐ ● Ⓒ Ⓓ

प्रश्न 2 Ⓐ Ⓑ ● Ⓓ

प्रश्न 3 Ⓐ ● Ⓒ Ⓓ

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।

6. सभी उत्तर केवल ओ०एम०आर० 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. ओ०एम०आर० 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।

महत्वपूर्णः प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्नपुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्नपुस्तिका प्राप्त कर लें।