

Roll. No.

Question Booklet Number

O.M.R. Serial No.

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

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

A

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 छॉटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

1. Cybersecurity refers to :
 - (A) Protecting hardware only
 - (B) Protecting data, systems, and networks
 - (C) Developing applications
 - (D) Internet usage
2. Which of the following is a cyber asset ?
 - (A) Data
 - (B) Hardware
 - (C) Software
 - (D) All of the above
3. Which goal ensures data is not disclosed to unauthorized users ?
 - (A) Integrity
 - (B) Availability
 - (C) Confidentiality
 - (D) Authentication
4. Integrity ensures :
 - (A) Data is always available
 - (B) Data is accurate and unchanged
 - (C) Data is hidden
 - (D) Data is deleted
5. Availability means :
 - (A) Data is always secure
 - (B) Data is accessible when needed
 - (C) Data is encrypted
 - (D) Data is hidden

1. 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
2. निम्नलिखित में से कौन-सी एक साइबर संपत्ति है ?
 - (A) डेटा
 - (B) हार्डवेयर
 - (C) सॉफ्टवेयर
 - (D) उपरोक्त सभी
3. कौन-सा लक्ष्य यह सुनिश्चित करता है कि डेटा अनधिकृत उपयोगकर्ताओं को प्रकट न हो ?
 - (A) अखंडता
 - (B) उपलब्धता
 - (C) गोपनीयता
 - (D) प्रमाणीकरण
4. 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
5. 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

6. CIA triad includes :
- (A) Confidentiality, Integrity, Availability
 (B) Control, Internet, Access
 (C) Code, Interface, Application
 (D) None of these
7. Authentication verifies :
- (A) Data accuracy
 (B) User identity
 (C) Network speed
 (D) File size
8. Authorization determines :
- (A) Who are you
 (B) What you can access
 (C) How data is stored
 (D) How fast system works
9. Non-repudiation ensures :
- (A) Data deletion
 (B) Sender cannot deny action
 (C) Fast access
 (D) Encryption
10. Which is NOT a security service ?
- (A) Authentication
 (B) Authorization
 (C) Compression
 (D) Confidentiality

6. CIA ट्रायड में शामिल हैं :
- (A) गोपनीयता, अखंडता, उपलब्धता
 (B) नियंत्रण, इंटरनेट, पहुँच
 (C) कोड, इंटरफ़ेस, एप्लिकेशन
 (D) इनमें से कोई नहीं
7. प्रमाणीकरण इसकी पुष्टि करता है :
- (A) डेटा की सटीकता
 (B) उपयोगकर्ता की पहचान
 (C) नेटवर्क की गति
 (D) फ़ाइल का आकार
8. 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
9. नॉन-रेप्यूडिएशन यह सुनिश्चित करता है :
- (A) डेटा हटाना
 (B) भेजने वाला अपने कार्य से इन्कार नहीं कर सकता
 (C) तेज़ पहुँच
 (D) एन्क्रिप्शन
10. इनमें से कौन-सी एक सुरक्षा सेवा नहीं है ?
- (A) प्रमाणीकरण
 (B) प्राधिकरण
 (C) संपीड़न
 (D) गोपनीयता

11. A threat is :
- (A) Protection mechanism
(B) Potential harm
(C) Security tool
(D) Software
12. Vulnerability is :
- (A) Strength
(B) Weakness in system
(C) Attack
(D) Tool
13. Risk is :
- (A) Threat × Vulnerability
(B) Data × Security
(C) Software × Hardware
(D) None of these
14. Which is an example of threat ?
- (A) Firewall
(B) Hacker
(C) Antivirus
(D) Encryption
15. Which is a vulnerability ?
- (A) Weak password
(B) Antivirus
(C) Backup
(D) Firewall

11. खतरा है :
- (A) सुरक्षा तंत्र
(B) संभावित नुकसान
(C) सुरक्षा उपकरण
(D) सॉफ्टवेयर
12. भेद्यता है :
- (A) शक्ति
(B) तन्त्र में कमजोरी
(C) हमला
(D) उपकरण
13. जोखिम है :
- (A) खतरा × भेद्यता
(B) डेटा × सुरक्षा
(C) सॉफ्टवेयर × हार्डवेयर
(D) इनमें से कोई नहीं
14. खतरे का एक उदाहरण कौन-सा है ?
- (A) फ़ायरवॉल
(B) हैकर
(C) एंटीवायरस
(D) एन्क्रिप्शन
15. इनमें से कौन-सी एक कमजोरी (vulnerability) है ?
- (A) कमजोर पासवर्ड
(B) एंटीवायरस
(C) बैकअप
(D) फ़ायरवॉल

16. White hat hackers are :
- (A) Criminals
(B) Ethical hackers
(C) Beginners
(D) Employees
17. Black hat hackers :
- (A) Protect systems
(B) Hack maliciously
(C) Test systems
(D) Secure networks
18. Grey hat hackers :
- (A) Always legal
(B) Mix of ethical and unethical
(C) Only criminals
(D) Beginners
19. Script kiddies are :
- (A) Experts
(B) Use ready-made tools
(C) Developers
(D) Engineers
20. Hacktivists are motivated by :
- (A) Money
(B) Learning
(C) Politics or ideology
(D) Fun
21. Malware stands for :
- (A) Malicious software
(B) Managed software
(C) Manual software
(D) Machine software
16. व्हाइट हैट हैकर्स होते हैं :
- (A) अपराधी
(B) एथिकल हैकर्स
(C) शुरूआती लोग
(D) कर्मचारी
17. 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
18. ग्रे हैट हैकर्स होते हैं :
- (A) हमेशा कानूनी
(B) नैतिक और अनैतिक का मिश्रण
(C) केवल अपराधी
(D) शुरूआती
19. स्क्रिप्ट किडीज़ होते हैं :
- (A) विशेषज्ञ
(B) बने-बनाए टूल्स का उपयोग करते हैं
(C) डेवलपर्स
(D) इंजीनियर
20. हैकटिविस्ट्स को किससे प्रेरणा मिलती है ?
- (A) पैसा
(B) सीखना
(C) राजनीति या विचारधारा
(D) मज़ा
21. Malware का अर्थ है :
- (A) दुर्भाग्यपूर्ण सॉफ्टवेयर
(B) प्रबंधित सॉफ्टवेयर
(C) मैनुअल सॉफ्टवेयर
(D) मशीन सॉफ्टवेयर

22. Virus is :

- (A) Hardware
- (B) Malware
- (C) Protocol
- (D) Network

23. Worm spreads :

- (A) Manually
- (B) Automatically
- (C) Offline
- (D) Slowly

24. Trojan horse is :

- (A) Safe software
- (B) Network
- (C) Firewall
- (D) Hidden malware

25. Spyware is used to :

- (A) Protect data
- (B) Monitor user activity
- (C) Delete files
- (D) Encrypt data

26. Antivirus is used to :

- (A) Attack system
- (B) Slow system
- (C) Delete OS
- (D) Detect malware

22. वायरस है :

- (A) हार्डवेयर
- (B) मैलवेयर
- (C) प्रोटोकॉल
- (D) नेटवर्क

23. वर्म फैलता है :

- (A) मैनुअली
- (B) ऑटोमैटिकली
- (C) ऑफ़लाइन
- (D) धीरे-धीरे

24. ट्रोजन हॉर्स है :

- (A) सुरक्षित सॉफ्टवेयर
- (B) नेटवर्क
- (C) फ़ायरवॉल
- (D) छिपा हुआ मैलवेयर

25. 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

26. 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

27. Firewall is used for :
- (A) Data storage
(B) Network protection
(C) Coding
(D) Gaming
28. Backup helps in :
- (A) Preventing attacks
(B) Encrypting files
(C) Speeding system
(D) Recovering data
29. Encryption provides :
- (A) Speed
(B) Security
(C) Storage
(D) Deletion
30. Password should be :
- (A) Simple
(B) Short
(C) Complex
(D) Same everywhere
31. Cybersecurity is important for :
- (A) Businesses
(B) Individuals
(C) Government
(D) All of the above
32. Data breach leads to :
- (A) Profit
(B) Data loss
(C) Speed
(D) Storage
27. फ़ायरवॉल का उपयोग किया जाता है :
- (A) डेटा स्टोरेज के लिए
(B) नेटवर्क सुरक्षा के लिए
(C) कोडिंग के लिए
(D) गेमिंग के लिए
28. 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
29. एन्क्रिप्शन प्रदान करता है :
- (A) गति
(B) सुरक्षा
(C) भंडारण
(D) विलोपन
30. पासवर्ड होना चाहिए :
- (A) सरल
(B) छोटा
(C) जटिल
(D) हर जगह एक जैसा
31. साइबर सुरक्षा किसके लिए महत्वपूर्ण है ?
- (A) व्यवसायों के लिए
(B) व्यक्तियों के लिए
(C) सरकार के लिए
(D) उपरोक्त सभी के लिए
32. डेटा ब्रीच से होता है :
- (A) लाभ
(B) डेटा की हानि
(C) गति
(D) स्टोरेज

33. Identity theft means :
- (A) Stealing identity
(B) Deleting files
(C) Hacking server
(D) Coding
34. Cybercrime includes :
- (A) Hacking
(B) Phishing
(C) Fraud
(D) All of the above
35. Which sector needs cybersecurity most ?
- (A) Banking
(B) Healthcare
(C) Education
(D) All of the above
36. Two-factor authentication uses :
- (A) One step
(B) Two methods
(C) No password
(D) Only OTP
37. Biometric authentication includes :
- (A) Password
(B) Fingerprint
(C) Username
(D) Email
33. पहचान की चोरी का अर्थ है :
- (A) पहचान चुराना
(B) फ़ाइल मिटाना
(C) सर्वर हैक करना
(D) कोडिंग
34. साइबर अपराध में शामिल हैं :
- (A) हैकिंग
(B) फ़िशिंग
(C) धोखाधड़ी
(D) उपरोक्त सभी
35. किस क्षेत्र को साइबर सुरक्षा की सबसे अधिक आवश्यकता है ?
- (A) बैंकिंग
(B) स्वास्थ्य सेवा
(C) शिक्षा
(D) उपरोक्त सभी
36. टू-फैक्टर ऑथेंटिकेशन में उपयोग होता है :
- (A) एक चरण
(B) दो तरीके
(C) कोई पासवर्ड नहीं
(D) केवल OTP
37. बायोमेट्रिक प्रमाणीकरण में शामिल है :
- (A) पासवर्ड
(B) फिंगरप्रिंट
(C) यूज़रनेम
(D) ईमेल

38. Digital signature ensures :
- (A) Speed
 - (B) Authenticity
 - (C) Storage
 - (D) Format
39. Risk management includes :
- (A) Ignoring threats
 - (B) Identifying threats
 - (C) Deleting files
 - (D) Formatting
40. Security policy is :
- (A) Rules for protection
 - (B) Software
 - (C) Hardware
 - (D) Network
41. Cybersecurity protects against :
- (A) Theft
 - (B) Damage
 - (C) Unauthorized access
 - (D) All of these
42. Ethical hacking is :
- (A) Illegal
 - (B) Legal testing
 - (C) Criminal activity
 - (D) Fraud
38. डिजिटल हस्ताक्षर सुनिश्चित करता है :
- (A) गति
 - (B) प्रामाणीकता
 - (C) भंडारण
 - (D) प्रारूप
39. जोखिम प्रबन्धन में शामिल होता है :
- (A) खतरों को नजरअंदाज करना
 - (B) खतरों को पहचानना
 - (C) फाइलो को डिलीट करना
 - (D) फार्मेटिंग
40. सुरक्षा नीति है :
- (A) सुरक्षा के नियम
 - (B) सॉफ्टवेयर
 - (C) हार्डवेयर
 - (D) नेटवर्क
41. साइबर सिक्योरिटी इनसे बचाती है :
- (A) चोरी
 - (B) नुकसान
 - (C) बिना इजाज़त के एक्सेस
 - (D) इनमे से सभी
42. एथिकल हैकिंग है :
- (A) अवैध
 - (B) कानूनी परीक्षण
 - (C) आपराधिक गतिविधि
 - (D) धोखाधड़ी

43. Patch management is used to :
- (A) Fix vulnerabilities
 (B) Delete files
 (C) Increase size
 (D) Format disk
44. Zero-day attack targets :
- (A) Known vulnerabilities
 (B) Unknown vulnerabilities
 (C) Hardware
 (D) Network cables
45. Insider threat comes from :
- (A) External hacker
 (B) Internal user
 (C) Antivirus
 (D) Firewall
46. Cyber hygiene refers to :
- (A) Cleaning computer
 (B) Safe practices
 (C) Formatting system
 (D) Deleting data
47. Strong security reduces :
- (A) Risk
 (B) Storage
 (C) Speed
 (D) Access
48. Cyber attack target :
- (A) Data
 (B) Systems
 (C) Networks
 (D) All of these

43. पैच मैनेजमेंट का उपयोग किया जाता है :
- (A) कमजोरियों को ठीक करने के लिए
 (B) फाइलों को हटाने के लिए
 (C) आकार बढ़ाने के लिए
 (D) डिस्क को फॉर्मेट करने के लिए
44. Zero-day attack के लक्ष्य हैं :
- (A) ज्ञात कमजोरियाँ
 (B) अज्ञात कमजोरियाँ
 (C) हार्डवेयर
 (D) नेटवर्क केबल
45. इनसाइडर थ्रेट आता है :
- (A) बाहरी हैकर से
 (B) आंतरिक उपयोगकर्ता से
 (C) एंटीवायरस से
 (D) फ़ायरवॉल से
46. साइबर हाइजीन का अर्थ है :
- (A) कम्प्यूटर की सफाई
 (B) सुरक्षित अभ्यास
 (C) सिस्टम को फॉर्मेट करना
 (D) डेटा को हटाना
47. कम्प्यूटर सुरक्षा कम करती है :
- (A) जोखिम
 (B) स्टोरेज
 (C) गति
 (D) पहुँच
48. साइबर हमले का निशाना होता है :
- (A) डेटा
 (B) सिस्टम
 (C) नेटवर्क
 (D) इनमें से सभी

49. Information security focuses on :
- (A) Protecting information
(B) Coding
(C) Gaming
(D) Hardware only
50. First step in security is :
- (A) Prevention
(B) Awareness
(C) Recovery
(D) Attack
51. 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
52. 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
53. A dangerous QR code often :
- (A) Opens unknown suspicious links
(B) Shows a wallpaper
(C) Opens camera
(D) Plays music
49. सूचना सुरक्षा किस पर केंद्रित है ?
- (A) सूचना की सुरक्षा पर
(B) कोडिंग पर
(C) गेमिंग पर
(D) केवल हार्डवेयर पर
50. सुरक्षा का पहला कदम है :
- (A) रोकथाम
(B) जागरूकता
(C) रिकवरी
(D) हमला
51. 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
52. 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 ढूँढने में
53. एक खतरनाक QR कोड अक्सर :
- (A) अनजान संदिग्ध लिंक खोलता है
(B) वॉलपेपर दिखाता है
(C) कैमरा खोलता है
(D) म्यूजिक बजाता है

54. 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
55. 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
56. Who can complain to the RBI Ombudsman ?
- (A) Only businessmen
 (B) Anyone having a banking issue
 (C) Only NRIs
 (D) Only RBI staff
57. 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
54. 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
55. 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
56. RBI ओम्बुड्समैन से कौन शिकायत कर सकता है ?
- (A) सिर्फ़ बिजनेसमैन
 (B) बैंकिंग समस्या वाला कोई भी व्यक्ति
 (C) सिर्फ़ NRI
 (D) सिर्फ़ RBI स्टाफ़
57. 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

58. 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
59. 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
60. 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
58. 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 वीडियो बना सकते हैं
59. डार्क वेब एक्सेस करने के लिए सबसे आम टूल कौन-सा है ?
- (A) TOR (द अनियन राउटर) ब्राउज़र
- (B) वाट्सएप
- (C) गुगल क्रोम
- (D) सफ़ारी
60. 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

Rough Work / रफ कार्य

Example :

Question :

Q.1 (A) ● (C) (D)

Q.2 (A) (B) ● (D)

Q.3 (A) ● (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.

Imp. 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) ● (C) (D)

प्रश्न 2 (A) (B) ● (D)

प्रश्न 3 (A) ● (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 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।

महत्वपूर्ण: 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।