NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT
Plot No. C-24, G Block, Bandra Kurla Complex
Bandra (E), Mumbai 400051

ADVERTISEMENT No. 04
RECRUITMENT OF SPECIALISTS ON CONTRACT – 2026-27 – CISO & DoS-CSITE

NABARD is an all-India Apex Organization, wholly owned by Government of India and an equal opportunity employer. NABARD invites **only ONLINE** applications, in the prescribed format, from Indian citizens, having necessary qualification and experience, for engagement of **16 Specialists on contract** for its **Head Office, Mumbai**. Candidates can apply **only ONLINE** on NABARD website www.nabard.org **between 09.10.2026** to **26.10.2026.**

Before applying, candidates should read all the instructions carefully and ensure that they fulfill all the eligibility criteria for the post. NABARD would admit candidates on the basis of the information furnished in the ONLINE application along with applicable requisite fee and shall verify their eligibility at the stage of interview / joining. If, at any stage, it is found that any information furnished in the ONLINE application is false/ incorrect or if according to the Bank, the candidate does not satisfy the eligibility criteria for the post, his/ her candidature will be cancelled, and he/she will not be allowed to appear for the interview / joining.

Candidates are requested to apply **only ONLINE** through Bank's website www.nabard.org. No other mode of submission of application will be accepted by NABARD. **ALL REVISIONS/ CORRIGENDUM (IF ANY) WILL BE HOSTED ON THE BANK'S WEBSITE ONLY.**

Help Facility: In case of any problem in filling up the form, payment of fee/intimation charges, complaints may be made at "Candidate Grievance Lodging and Redressal Mechanism" at https://cgrs.ibps.in/. Do not forget to mention **"NABARD – Recruitment to the post of Specialists on contract"** in the subject of the email.

Important Dates / Timelines

Online Application Registration and Payment of Online Fees/Intimation Charges	**09.10.2026 to 26.10.2026**
NABARD reserves the right to make change in the dates indicated above.	

I. NUMBER OF VACANCIES AND RESERVATION

Department Name	Sr. No.	Name of the post	SC	ST	OBC	EWS	UR	Total
Chief Information Security Office (CISO)	1	SOC (Security Operations Centre) Analyst	0	0	0	0	03	**03**
	2	Information Security Analyst	0	0	0	0	03	**03**
	3	Network Security Analyst	0	0	0	0	01	**01**
	4	Ethical Hacker & Penetration Tester	0	0	0	0	01	**01**
Department of Supervision (DoS) - CSITE	5	Lead Auditor	0	0	01	0	01	**02**
	6	Cyber & Network Security Specialist	0	0	0	0	02	**02**
	7	IT Infrastructure & Banking Specialist	0	0	0	0	02	**02**
	8	Cyber Security Analyst	0	0	0	0	02	**02**
Total			**0**	**0**	**01**	**0**	**15**	**16**

II. Place of posting - MUMBAI

III. ELIGIBILITY CRITERIA: Educational Qualification, Experience and Job Profile (as on 01.10.2026)

1. SOC (Security Operations Centre) Analyst

Age	24 - 35 years
Qualification	**Mandatory** • BE /B.Tech in Computer Science/ Computer Engineering/ Information Technology/ Electronics & Communication/ Information Science/ Electrical/ Cyber Security; OR • MCA; OR Post Graduate degree in Computer Science / Information Technology/ Cyber Security/ Information Security/ Computer Engineering/ Information Systems/ Software Engineering/ Electronics & Communication Engineering (minimum of 60% marks or equivalent grade) **Mandatory Certification** Any one of the following: • CompTIA Security+ • CEH (Certified Ethical Hacker) • Equivalent cyber security certification

	Desirable Certification • SIEM tool certification (relevant to any SIEM platform) • CHFI / CySA+ / Blue Team certifications
Experience	**Mandatory** • Minimum 3 years of post qualification experience in IT / Cyber Security roles, including handling security solutions and security risk identification **Desirable** • Experience in SOC operations as an analyst, preferably in large organizations / BFSI / managed SOC environments
Job profile	**Key accountabilities/ KRAs/ KPIs:** • Perform 24×7 monitoring of security events, including SIEM alerts, logs, and endpoint activity. • Detect, analyse, and escalate security incidents in accordance with defined procedures. • Conduct incident triage, analysis, and initial investigation, and support containment and remediation activities. • Assist in incident response and root cause analysis (RCA), including preparation of incident reports. • Analyse logs and telemetry data to identify anomalies, suspicious behaviour, and potential threats. • Correlate events across systems to provide consolidated threat visibility. • Support investigation of security incidents, including analysis of logs, endpoints, and network traffic. • Assist in analysis of malicious activity and artifacts, including malware indicators, scripts, and suspicious binaries, and coordinate with specialised teams where deeper analysis is required. • Operate and support security monitoring tools, including SIEM, EDR, antivirus, and related technologies. • Monitor KRIs and security trends, and support early warning identification. • Prepare and maintain incident reports, dashboards, and security documentation. • Participate in threat monitoring, cyber drills, and SOC review exercises. • Coordinate with vendors and internal teams for incident resolution and follow up actions. • The role may require working in rotational shifts to support 24×7 SOC operations. • Perform any other cyber security responsibilities assigned by the Bank.

2. Information Security Analyst

Age	24 - 35 years
Qualification	**Mandatory** • BE /B.Tech in Computer Science/ Computer Engineering/ Information Technology/ Electronics & Communication/ Information Science/ Electrical/ Cyber Security;OR • MCA; OR Post Graduate degree in Computer Science / Information Technology/ Cyber Security/ Information Security/ Computer Engineering/ Information Systems/ Software Engineering/ Electronics & Communication Engineering (minimum of 60% marks or equivalent grade) **Mandatory Certifications** Any one of the following: • CISA • CISM • CISSP • Equivalent certification in Information Security / IT Risk / Compliance **Desirable Certification** Certifications in • CRISC / CGEIT • ISO 27001 Lead Implementer / Lead Auditor • PCI DSS / IT Governance / Risk certifications • Cloud security certifications (CCSP / AWS / Azure Security)
Experience	**Mandatory** • Minimum 2–4 years of post qualification experience in Information Security / IT Risk / Cyber Security roles, including involvement in security assessment, risk identification, compliance, or governance activities **Desirable** Experience in IT Risk, Information Security governance, audits, or compliance functions, preferably in: • Banking / Financial Services / Insurance (BFSI) sector • Cyber Security organizations / SOC environments • IT consulting firms (including CERT In empanelled organisations) • FinTech environments • Experience in a combination of technical and governance roles will be considered an advantage.
Job profile	**Key accountabilities/ KRAs/ KPIs** • The role supports IT risk assessment, security governance, regulatory compliance, and security assurance functions, with working knowledge of technical security domains.

	• Conduct IT and cyber risk assessments, identify control gaps, and support implementation of risk mitigation measures. • Support security governance and compliance activities, including policy review, exception handling, and adherence to internal frameworks and regulatory requirements. • Coordinate with departments for audit, inspection, and regulatory compliance, including preparation of responses, evidence collation, and tracking of action taken reports (ATR). • Monitor and analyse Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), and support preparation of periodic security reports and dashboards. • Provide security assurance for IT projects and systems, including review of architecture, configurations, and security controls for applications, infrastructure, APIs, and integrations. • Analyse security posture of applications and IT infrastructure, including access controls, network permissions, and exposure risks. • Support review of cloud environments and modern IT architectures, including virtualization, containerization, APIs, and microservices, from a security standpoint. • Assist in assessment of security threats related to remote access solutions, new IT products, and technology deployments. • Support security architecture reviews and design validation, providing inputs on secure implementation across platforms and environments. • Assist in third party and external partner security oversight, including monitoring compliance with security standards and reporting status to management. • Support evaluation and implementation of cyber security solutions, including analysis of suitability, effectiveness, and alignment with organisational requirements. • Coordinate with SOC, network, and development teams to ensure consistent implementation of security controls and risk mitigation measures. • Participate in security audits, risk reviews, awareness initiatives, and compliance programmes across the organisation. • Provide inputs for security documentation, policies, standards, and guidelines, and support continuous improvement of the organisation's security posture. • Possess working knowledge of technical security domains, including network security, application security, and cloud security concepts. • Perform any other information and cyber security responsibilities assigned by the Bank from time to time.

3. Network Security Analyst

Age	26 - 38 years
Qualification	**Mandatory** • BE /B.Tech in Computer Science/ Computer Engineering/ Information Technology/ Electronics & Communication/ Information Science/ Electrical/ Cyber Security; OR MCA; OR Post Graduate degree in Computer Science / Information Technology/ Cyber Security/ Information Security/ Computer Engineering/ Information Systems/ Software Engineering/ Electronics & Communication Engineering (minimum of 60% marks or equivalent grade) **Mandatory Certifications** Any one of the following: • CCNP Security • Equivalent certification in network / infrastructure security **Desirable Certification** • CISSP / CISM • OEM certifications such as Check Point (CCSA/CCSE), Palo Alto (PCNSE), Fortinet (NSE) • Cloud security certifications (CCSP / AWS / Azure Security)
Experience	**Mandatory** • 5 years of IT experience and minimum 3 years of post-qualification work experience in network security in handling security solutions and various Information Security related roles including Network Security, identifying security risk and development plan. **Desirable** • Preference will be given to candidate with work experience in large organizations/ Cyber Security Operations Centre with Banking / Financial Services/ Insurance Sector (BFSI) experience.
Job profile	**Key accountabilities/ KRAs/ KPIs** • Implement, manage, and maintain network security infrastructure, including firewalls, IPS/IDS, WAF, NAC, NBAD, Anti-DDoS, and related security solutions. • Monitor network security systems and analyse logs, alerts, and events to detect suspicious activities and potential security threats. • Investigate security incidents, identify breaches, and support containment and remediation actions, including root cause analysis. • Correlate security events across network infrastructure to provide holistic threat visibility and support risk identification.

	• Perform configuration review, hardening, and optimisation of network security devices to ensure effectiveness of security controls. • Support change management and validation for network security configurations, including firewall rules, access controls, and exposure management. • Ensure health monitoring, performance validation, and availability of network security devices, including backup verification and disaster recovery readiness. • Conduct periodic reviews of network security posture, including vulnerabilities, misconfigurations, and exposure risks. • Coordinate with OEMs and system integrators for issue resolution, upgrades, patching, and RMA support, where required. • Prepare and maintain reports, security assessments, and dashboards to support policy improvements and management decisions. • Support monitoring of emerging threats, attack patterns, and network-level risks, and recommend appropriate control enhancements. • Collaborate with SOC, IT, and application teams for incident resolution, implementation of controls, and strengthening of overall security posture. • Participate in security audits, reviews, and cyber drills, as required. • The role may involve participation in on-call / extended support for critical network security incidents. • The role may require working in rotational shifts or extended hours, as required, to support critical network security operations. • Perform any other security-related responsibilities as assigned by the Bank.

4. Ethical Hacker & Penetration Tester

Age	25 - 35 years
Qualification	**Mandatory** • BE /B.Tech in Computer Science/ Computer Engineering/ Information Technology/ Electronics & Communication/ Information Science/ Electrical/ Cyber Security; • OR MCA; OR Post Graduate degree in Computer Science / Information Technology/ Cyber Security/ Information Security/ Computer Engineering/ Information Systems/ Software Engineering/ Electronics & Communication Engineering (minimum of 60% marks or equivalent grade) **Mandatory Certifications** Any one of the following: • CEH (Certified Ethical Hacker) • OSCP (Offensive Security Certified Professional) • ECSA (EC Council Certified Security Analyst) • Equivalent certification in penetration testing / offensive security

	Desirable Certification • GWAPT (Web Application Penetration Tester) • GPEN (GIAC Penetration Tester) • OSWE / OSWA (Offensive Security Web Certifications) • Any specialised application / API security certification
Experience	**Mandatory** • Minimum 2–4 years of post qualification experience in Vulnerability Assessment and Penetration Testing (VAPT) / Ethical Hacking, including hands on experience in application, API, and infrastructure security testing. **Desirable** Experience in: • Banking / Financial Services / Insurance (BFSI) sector • CERT In empanelled organisations / security consulting firms • Red teaming or advanced penetration testing assignments
Job profile	**Key accountabilities/ KRAs/ KPIs** • Conduct vulnerability assessment and penetration testing (VAPT) across applications, APIs, networks, and infrastructure. • Perform ethical hacking, red teaming, and security assessments to identify vulnerabilities, attack vectors, and potential exploitation paths. • Execute application and API security testing, including dynamic testing (DAST), secure configuration reviews, and validation of implemented controls. • Identify security weaknesses, classify risks, and provide actionable remediation recommendations. • Support re validation and closure of vulnerabilities, ensuring reduction of repeat findings and improvement in overall security posture. • Perform basic threat simulation and adversarial testing, where required. • Assist in review of secure configurations, security controls, and architecture from a vulnerability and exposure assessment perspective. • Analyse test results and prepare detailed VAPT reports, risk assessments, and management summaries. • Support pre go live security testing and validation for new applications and system changes. • Coordinate with internal teams and vendors for remediation tracking and closure of identified vulnerabilities. • Support evaluation of new tools, testing techniques, and security practices to enhance testing capability. • Participate in security audits, assessments, and compliance activities as required. • The role may require working in extended hours based on testing

	schedules and project timelines. • Possess strong hands-on skills in common VAPT tools and methodologies (e.g., Burp Suite, OWASP testing techniques), where applicable. • Perform any other information and cyber security responsibilities assigned by the Bank.

5. Lead Auditor

Age	32 - 45 years
Qualification	**Mandatory** • B.E./B. Tech in Computer Science and Engineering (CSE), Electronics and Communication Engineering (ECE), or Information Technology (IT); OR • Bachelor's Degree in any discipline with a Master's degree in Computer Science/IT / ECE **Mandatory Certifications** CISA (Mandatory), plus at least one of the following: • CISSP • ISO 27001 Lead Auditor • Lead Implementer and CISA
Experience	**Experience** • Minimum 8 years of overall IT experience, including at least 5 years conducting technology/IS audits in the BFSI sector, with experience leading audit teams. Experience, certification, or training in Cloud Audit, Project Management, and PCI-DSS is preferred.
Job profile	**Key accountabilities/ KRAs/ KPIs** • Design, develop, and maintain audit management processes including schedules, reports, checklists, and procedures. • Monitor and review RBI and NABARD circulars, advisories, and alerts, and incorporate them into audit checklists. • Coordinate and facilitate audit activities with onsite teams, inspected banks, regional offices, and head office. • Conduct audits, prepare reports, and ensure timely review and closure of audit findings. • Track audit report status and escalate issues based on defined timelines. • Generate MIS reports, analyse inspection trends, and present findings to senior management. • Identify and improve existing audit methodologies and processes. • Ensure continuous improvement in audit processes to maintain cyber security compliance. • Prepare and disseminate advisories and alerts and monitor and follow up on compliance.

	• Stay updated with new cyber security regulations, technologies, and developments. • Provide training to staff. • Travel across the country for audit assignments. • Other CSITE-related work as assigned by management.

6. Cyber & Network Security Specialist

Age	30 - 45 years
Qualification	**Mandatory** • B.E./B.Tech in Computer Science and Engineering (CSE), Electronics and Communication Engineering (ECE), or Information Technology (IT); OR • Bachelor's degree in any discipline with a Master's in Computer Science/IT/ECE **Mandatory Certifications** CISA (Mandatory), plus at least one of the following: • CCNA (Cisco Certified Network Associate) • CCNP (Cisco Certified Network Professional) • CEH (Certified Ethical Hacker) • CISM (Certified Information Security Manager)
Experience	**Experience** • Minimum 6 years handling network devices (firewalls, routers, switches), cyber security consulting, ISMS management, SOC/VAPT; including at least 3 years in technology/IS audit. Experience, certification, or training in network/cyber security auditing, IT audits, or IT risk assessment is preferred.
Job profile	**Key accountabilities/ KRAs/ KPIs** • Conduct audits on network security, firewalls, encryption, incident response, and other cyber-related areas. • Prepare, update, and review network-related checklists, questionnaires, returns, and procedures. • Monitor and review RBI and NABARD circulars, advisories, and alerts, and incorporate them into audit checklists. • Prepare and disseminate advisories and alerts, and monitor and follow up on compliance. • Review security processes, policies, and compliance. • Prepare reports, corrective action reviews, and audit documentation. • Stay updated on international standards, threats, and vulnerabilities. • Travel required for audits across the country. • Provide training to staff. • Other CSITE-related work as assigned by management.

7. IT Infrastructure & Banking Specialist

Age	30 - 45 years
Qualification	**Mandatory** • B.E./B.Tech in Computer Science and Engineering (CSE), Electronics and Communication Engineering (ECE), or Information Technology (IT); OR • Bachelor's degree in any discipline with a Master's in Computer Science/IT/ECE **Mandatory Certifications** CISA (Mandatory), plus at least one of the following: • CISM (Certified Information Security Manager) • ISO 27001 Lead Auditor • PCI DSS implementation certification (PCIP/ ISA/QSA/CPISI)
Experience	**Experience** • Minimum 6 years handling CBS and payment channels (SWIFT, ATM, Internet/Mobile Banking, NEFT/RTGS/UPI/IMPS), IT infrastructure, and virtualization; including at least 3 years in technology/IS audit
Job profile	**Key accountabilities/ KRAs/ KPIs** • Conduct audits on CBS, payment systems, vendor onboarding, SLAs, BCP, and other cyber-related areas. • Review IT infrastructure and cyber security compliance. • Prepare and disseminate advisories and alerts and monitor and follow up on compliance. • Prepare audit reports, checklists, and corrective action reviews. • Monitor and review RBI and NABARD circulars, advisories, and alerts, and incorporate them into audit checklists. • Stay updated on international standards, threats, and vulnerabilities. • Provide training to staff. • Travel required for audits across the country. • Other CSITE-related work as assigned by management.

8. Cyber Security Analyst

Age	24 - 32 years
Qualification	**Mandatory** • B.E./B.Tech in Computer Science and Engineering (CSE), Electronics and Communication Engineering (ECE), or Information Technology (IT); OR • Bachelor's degree in any discipline with a Master's in Computer Science/IT/ECE **Mandatory Certifications** At least one of the following:

	• CEH (Certified Ethical Hacker) • ISO 27001 Lead Auditor • Database Certification (Oracle/ Microsoft SQL) • Cloud Certification (AWS / GCP / Microsoft Azure/ Oracle)
Experience	**Experience** • Minimum 3 years in IT or cyber security.
Job profile	**Key accountabilities/ KRAs/ KPIs** • Associating with the audit team. • Review compliance processes and identify gaps. • Performing desk scrutiny of returns and reports. • Stay updated on security standards and vulnerabilities. • MIS management. • Prepare and disseminate advisories and alerts and monitor and follow up on compliance. • Coordination with banks. • Travel required for audits across the country. • Other CSITE-related work as assigned by management.

IV Selection Process

1) The selection will be by way of interview. The candidates will be shortlisted for interview in the ratio of 1:3 on the basis of qualification, experience, etc.

2) The shortlisted candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalized Banks and Financial Institutions are advised to submit 'No Objection Certificate' from their employer at the time of interview, failing which their candidature may not be considered and travelling expenses, if any, otherwise admissible, will not be paid.

3) Selected candidates will have to undergo pre-recruitment medical examination. Final appointment will be done only of those candidates who are declared medically fit by Bank's Medical Officer.

4) The Bank reserves the right to increase/ decrease the number of post/s or cancel the above contract recruitment in part or full as per institutional requirement without assigning any reason. The roll numbers of candidates shortlisted for interview & subsequent selection shall be published on Bank's website viz. www.nabard.org. The decision of the Bank in shortlisting candidates for interview & selecting them for appointment based on minimum qualifying standard shall be final and no correspondence will be entertained in this regard. The final appointment will be based on the decision of the Selection Committee constituted for the purpose.

V. APPLICATION FEE (NON-REFUNDABLE)

Application fee (exclusive of applicable GST) for the post will be as under:

(Amount in Rs.)

Category of applicant	Application Fee	Intimation charges etc.	Total
For SC/ ST/ PWBD	NIL	150	150*
For all others	700	150	850*

* Exclusive of applicable GST

VI. Place of posting, Compensation, Period of contract and other benefits:

a. Place of Posting : NABARD, Head Office, Mumbai

b. Compensation

Sr No	Post	Consolidated Remuneration All inclusive (in Rs.)
1	SOC (Security Operations Centre) Analyst	12-18 lakh/pa
2	Information Security Analyst	12-18 lakh/pa
3	Network Security Analyst	18–25 lakh/pa
4	Ethical Hacker & Penetration Tester	15-24 lakh/pa
5	Lead Auditor	35-40 lakh/pa
6	Cyber & Network Security Specialist	30-35 lakh/pa
7	IT Infrastructure & Banking Specialist	30-35 lakh/pa
8	Cyber security Analyst	18-20 lakh/pa

The Specialist on contract will be liable for tax liabilities as per Income Tax Act & Rules in force and the tax will be deducted at source. The amount of compensation being cost to NABARD, will be inclusive of any statutory payments that NABARD may be required to pay on behalf of the Specialist on contract. Annual increment up to a maximum of 10% can be granted based on satisfactory performance and discretion of the Bank.

c. Period of contract

i. 02 years from the date of appointment extendable for a further period of 03 years. The engagement would be extended after taking a review one year at a time and in any case will not be beyond 05 years. The Bank may terminate the contract at any time without prior notice and without providing any reason thereof. However, in normal course, NABARD may terminate the engagement by giving one month's notice in advance. The Specialist can also seek termination of the contract by giving one month's notice.

ii. In case the notice period is not being served, the Specialist has to pay a sum equivalent to pay for the period of notice required of him /her.

iii. Notwithstanding the above, NABARD retains the right to modify the terms of the recruitment, suspend or terminate the engagement with any Specialist, without assigning any reason thereof.

d. Superannuation Benefits

The Specialists shall not be entitled to any superannuation benefits viz., Provident Fund, Pension, Gratuity, etc.

e. Travelling / Halting Allowance

Whenever official tour is required, the Specialist will be entitled for Travelling & Halting Allowance as admissible to the officers in the Bank of equivalent grade for official tours outside the headquarters or as mentioned in the appointment letter.

f. Leave

i. Maximum of 30 days per calendar year during the contract period, on a proportionate basis.
ii. The total absence during contract period cannot be beyond 10 days at any point of time except on emergency medical grounds subject to production of relevant medical certificate.
iii. If absence during contract period is more than 01 month, it shall be treated as notice period except under exceptional circumstances where leave is duly approved by the concerned department's CGM/OIC.
iv. During the notice period, the Specialists on Contracts may not be allowed to avail leave. However, he/ she may be allowed to avail leave only on emergency medical grounds subject to production of relevant medical certificate.
v. Contract appointees will be permitted to avail leave subject to administrative convenience of the Bank.
vi. Un-availed leave at the end of a year will not be permitted to be carried forward.
vii. Intervening holidays during the period of absence will be reckoned as leave.
viii. Any absence beyond the above period may be treated as leave without pay.

g. Accommodation:

i. Specialist will be allotted quarters based on his/her request and subject to availability, against payment of licence fee of 0.5% of remuneration.

ii. Specialist will be eligible for a fixed House Rent Allowance (HRA) of 10% of remuneration in the event of non-allotment of quarters.

h. Reporting:

The Specialist will report to an officer of higher grade in the department as decided by OIC.

i. Office Facilities:

i. NABARD will provide Office Space, Internet Connectivity, and other support facilities.

ii. Lounge facilities as applicable to the officers of the Bank will be provided. This facility will not be applicable in case of remote working.

j. **Medical Facility :**

For self only, at the Dispensary of the Bank, wherever available.

k. Legal Status:

Specialist shall be selected on contract basis and shall have no right / claim for placement in NABARD by the virtue of engagement of their services by the Bank. Services of the staff on contract shall be governed by the code of conduct as applicable to Specialists / Consultants engaged on contract.

VII. How to apply:

Detailed Guidelines/Procedures for

a. Application Registration
b. Payment of fees
c. Document scan and upload

Candidates can apply only online from 09.10.2026 to 26.10.2026 and no other mode of application will be accepted.
Important Points to be noted before registration.

Before applying online, candidates should-

1. Scan their:
   a. Photograph (4.5cm × 3.5cm)
   b. Signature (with black ink)
   c. Left thumb impression (on white paper with black or blue ink)
   d. A handwritten declaration (on a white paper with black ink) (text given below)
   e. Ensuring that all these scanned documents adhere to the required specifications as mentioned at point VIII C.

2. The left thumb impression should be properly scanned and not smudged. (If a candidate is not having left thumb, he/she may use his/ her right thumb for applying.)

3. The text for the handwritten declaration is as follows –

   "I, _(Name of the candidate), hereby declare that all the information submitted by me in the application form is correct, true and valid. I will present the supporting documents as and when required."

   The above-mentioned handwritten declaration has to be in the candidate's own handwriting and in English only. If it is written and uploaded by anybody else or in any other language, the application will be considered as invalid. (In the case of Visually Impaired candidates who cannot write may get the text of declaration typed and put their

left-hand thumb impression below the typed declaration and upload the document as per specifications.)

4. Keep the necessary details/documents ready to make Online Payment of the requisite application fee/ intimation charges.

5. Have a valid personal email ID and mobile number, which should be kept active till the completion of this Recruitment Process. Bank may send intimation to download call letters for the Examination etc. through the registered e-mail ID. In case a candidate does not have a valid personal e-mail ID, he/she should create his/her new e-mail ID and mobile number before applying on-line and must maintain that email account and mobile number.

Application fees/ intimation charges (nonrefundable) payment of fee online: 09.10.2026 to 26.10.2026

Bank Transaction charges for Online Payment of application fees/intimation charges will have to be borne by the candidate.

A. Application Registration

a. Candidates to visit the NABARD website – www.nabard.org and under Career Notices, click on the option "APPLY HERE" below the concerned recruitment advertisement, which will open a new screen.

b. To register application, choose the tab "Click here for New Registration" and enter Name, Contact details and Email-id. A Provisional Registration Number and Password will be generated by the system and displayed on the screen. Candidate should note down the Provisional Registration Number and Password. An Email & SMS indicating the Provisional Registration number and Password will also be sent.

c. In case any candidate is unable to complete the application form in one go, he / she can save the data already entered by choosing "SAVE AND NEXT" tab. **Prior to submission of the online application, candidates are advised to use the "SAVE AND NEXT" facility to verify the details in the online application form and modify the same if required**. Visually Impaired candidates should fill the application form carefully and verify/ get the details verified to ensure that the same are correct prior to final submission.

d. Candidates are advised to carefully fill and verify the details filled in the online application themselves as no change will be possible/ entertained after clicking the COMPLETE REGISTRATION BUTTON.

e. The Name of the candidate or his /her Father/ Husband etc. should be spelt correctly in the application as it appears in the Certificates/ Mark sheets/Identity proof. Any change/alteration found may disqualify the candidature.

f. Validate your details and save your application by clicking the 'Validate your details' and 'Save & Next' button.

g. Candidates can proceed to upload Photo & Signature as per the specifications given in the Guidelines for Scanning and Upload of Photograph and Signature detailed under point "C".

h. Candidates can proceed to fill other details of the Application Form.

i. Click on the Preview Tab to preview and verify the entire application form before FINAL SUBMIT.

j. Modify details, if required, and click on 'COMPLETE REGISTRATION' ONLY after verifying and ensuring that the photograph, signature uploaded and other details filled by you are correct.

k. Click on 'Payment' Tab and proceed for payment.

B. Payment of Fees
Online Mode

a. The application form is integrated with the payment gateway and the payment process can be completed by following the instructions.

b. The payment can be made by using Debit Cards (RuPay/Visa/MasterCard/Maestro), Credit Cards, Internet Banking, IMPS, Cash Cards/ Mobile Wallets.

c. After submitting your payment information in the online application form, **PLEASE WAIT FOR THE INTIMATION FROM THE SERVER. DO NOT PRESS BACK OR REFRESH BUTTON IN ORDER TO AVOID DOUBLE CHARGE**

d. On successful completion of the transaction, an e-Receipt will be generated.

e. Non-generation of 'E-Receipt' indicates PAYMENT FAILURE. On failure of payment, Candidates are advised to login again using their Provisional Registration Number and Password and repeat the process of payment.

f. Candidates are required to take a printout of the e-Receipt and online Application Form containing fee details. Please note that if the same cannot be generated, online transaction may not have been successful.

g. For Credit Card users: All charges are listed in Indian Rupee. If you use a non-Indian credit card, your bank will convert to your local currency based on prevailing exchange rates.

h. To ensure the security of your data, please close the browser window once your transaction is completed.

i. There is facility to print application form containing fee details after payment of fees.

C. Guidelines for scanning and Upload of Documents

Before applying online a candidate will be required to have a scanned (digital) image of his/her photograph, signature, left thumb impression and the hand written declaration as per the specifications given below.

Photograph Image: (4.5cm × 3.5cm)

a. Photograph must be a recent passport style colour picture.
b. Make sure that the picture is in colour, taken against a light-coloured, preferably white, background.
c. Look straight at the camera with a relaxed face
d. If the picture is taken on a sunny day, have the sun behind you, or place yourself in the shade, so that you are not squinting and there are no harsh shadows
e. If you have to use flash, ensure there's no "red-eye"
f. If you wear glasses make sure that there are no reflections and your eyes can be clearly seen.
g. Caps, hats and dark glasses are not acceptable. Religious headwear is allowed but it must not cover your face.
h. Dimensions 200 x 230 pixels (preferred)
i. Size of file should be between 20kb–50 kb
j. While scanning the photograph ensure that the size of the scanned image is not more than 50kb. If the size of the file is more than 50 kb, then adjust the settings of the scanner such as the DPI resolution, colours, etc.

Live Photograph Capture

a. In addition to the above photograph, candidates will also be required to capture and upload their live photograph either by using webcam or mobile phone.
b. On selecting “Capture Photo” option, candidates’ webcam will be activated allowing them to click their picture, which will get auto uploaded in the application form.
c. On selecting “Click here to Scan” option, candidates can use their mobile phone to scan the QR code, which will redirect to a website, allowing to click photograph on their mobile phone. On selecting the taken picture, photograph will get auto uploaded in the application form.

Do’s and Don’ts of Photo Capture

Dos:

- Ensure the photo is captured against a light coloured, preferably white background and there is adequate light.
- Look straight at the webcam/ camera.
- Photograph should be of passport size.

Don’ts:

- Small size photograph not to be clicked/ uploaded.
- Coloured glasses or sunglasses/ Cap should not be worn.
- Shadow on face/ not facing the camera/ distorted face/ face covered with mask / blurred image.
- Photo not taken in dark/ improper background.

Signature, left thumb impression and hand-written declaration Image:
Signature

a. The applicant has to sign on white paper with Black Ink pen.
b. Dimensions 140 x 60 pixels (preferred)
c. Size of file should be between 10kb – 20kb for signature and 20kb - 50kb for left thumb impression.
d. Ensure that the size of the scanned image is not more than 20kb

Left Thumb
The applicant has to put his left thumb impression on a white paper with black or blue ink.

a. File type: jpg / jpeg
b. Dimensions: 240 x 240 pixels in 200 DPI (Preferred for required quality) i.e 3 cm * 3 cm (Width * Height)
c. File Size: 20 KB – 50 KB

Hand written declaration
a. The applicant has to write the declaration in English clearly on a white paper with black ink.
b. File type: jpg / jpeg
c. Dimensions: 800 x 400 pixels in 200 DPI (Preferred for required quality) i.e 10 cm * 5 cm (Width * Height)
d. File Size: 50 KB – 100 KB
e. The signature, left thumb impression and the hand written declaration should be of the applicant and not by any other person.
f. Hand written declaration in CAPITAL LETTERS shall NOT be accepted

Scanning the documents:
a. Set the scanner resolution to a minimum of 200 dpi (dots per inch)
b. Set Colour to True Colour
c. File Size as specified above
d. Crop the image in the scanner to the edge of the photograph/signature/ left thumb impression / handwritten declaration, then use the upload editor to crop the image to the final size (as specified above).
e. The image file should be JPG or JPEG format. An example file name is: image01.jpg or image01.jpeg. Image dimensions can be checked by listing the folder files or moving the mouse over the file image icon.
f. Candidates using MS Windows/MS Office can easily obtain documents in .jpeg format by using MS Paint or MS Office Picture Manager. Scanned documents in any format can be saved in .jpg/ .jpeg format by using 'Save As' option in the File menu. Size can be adjusted by using crop and then resize option.

Uploading latest C.V./Resume and Proof of current Cost to Company in the specified field.
a. Applicant has to upload the latest C.V/Resume and Proof of current Cost to Company in .pdf format.
b. Max. File Size: 500 KB.

Procedure for uploading the documents

a. While filling in the Online Application Form the candidate will be provided with separate links for uploading Photograph, signature, left thumb impression and hand written declaration
b. Click on the respective link "Upload Photograph / signature / Upload left thumb impression / hand written declaration"
c. Browse and Select the location where the Scanned Photograph / signature / left thumb impression / hand written declaration file has been saved.
d. Select the file by clicking on it
e. Click the 'Open/Upload'
f. If the file size and format are not as prescribed, an error message will be displayed.
g. Preview of the uploaded image will help to see the quality of the image. In case of unclear / smudged, the same may be re-uploaded to the expected clarity /quality.
h. Your Online Application will not be registered unless you upload your Photograph, signature, left thumb impression and hand written declaration as specified.

Note:

a. In case the face in the photograph or signature or left thumb impression or the hand written declaration is unclear / smudged then the candidate's application may be rejected.
b. After uploading the Photograph / signature / left thumb impression / hand written declaration in the online application form candidates should check that the images are clear and have been uploaded correctly. In case the photograph or signature or left thumb impression or the hand written declaration is not prominently visible, the candidate may edit his/ her application and re-upload his/ her photograph or signature or left thumb impression or the hand written declaration, prior to submitting the form.
c. Candidate should also ensure that photo is uploaded at the place of photo and signature at the place of signature. If photo in place of photo and signature in place of signature is not uploaded properly, candidate will not be allowed to appear for the interview.
d. Candidate must ensure that Photo to be uploaded is of required size and the face should be clearly visible.
e. If the photo is not uploaded at the place of Photo Admission for Examination will be rejected/denied. Candidate him/herself will be responsible for the same.
f. Candidates should ensure that the signature uploaded is clearly visible
g. After registering online candidates are advised to take a printout of their system generated online application forms.

D. Action against candidates found guilty of misconduct/ use of unfair means.

Candidates are advised in their own interest that they should not furnish any particulars that are false, tampered with or fabricated and should not suppress any material information while submitting online application. At the time of interview or in a subsequent selection procedure, if a candidate is (or has been) found guilty of –

a. using unfair means or
b. impersonating or procuring impersonation by any person or

c. resorting to any irregular or improper means in connection with his/ her candidature or
d. obtaining support for his/ her candidature by unfair means.

General Instructions

a. Depending upon the requirement, the Bank reserves the right to increase/decrease/modify/cancel/restrict/curtail/enlarge any or all the provisions of the vacancy/ the recruitment process, if need arises, without any further notice and without assigning any reason therefor.

b. The Specialist shall have no right or claim for regular employment in the organization.

c. No correspondence will be entertained from any ineligible and non-selected candidate. In all matters regarding eligibility, the selection process, the stages at which the scrutiny of eligibility is to be undertaken, documents have to be produced for the selection process, assessment, prescribing minimum qualifying standards in the selection process, number of vacancies, communication of results, etc., the Bank's decision shall be final and binding on the candidates and no correspondence shall be entertained in this regard.

d. Any legal proceedings in respect of any matter of claim or dispute arising out of this advertisement and/ or an application in response thereto can be instituted only in Mumbai, and courts/ tribunals/ forums at Mumbai only shall have sole & exclusive jurisdiction to try any clause/ dispute.

e. Any notice/communication meant for the candidates displayed on the Bank's website, sent by Registered/Speed Posts, or conveyed to the email id mentioned in the application at the time of registration with the Bank, shall be deemed to be sufficient service of communication upon the candidate, for all purposes.

Note:

In case of any corrigendum issued on the above advertisement and further announcements, it will be published only on Bank's website www.nabard.org.

IMPORTANT DATES

Online Application Registration and Payment of Online Fees/ Intimation Charges.	**09.10.2026 to 26.10.2026**

Place: Mumbai
Date: 09 October 2026

Chief General Manager
HRMD, Head Office, Mumbai