State Bank of India

Central Recruitment & Promotion Department
Corporate Centre, Mumbai
Email: crpd@sbi.co.in

SBI SHINES GOLD WINNER IN 4 CATEGORIES IN ECONOMICS TIMES HUMAN CAPITAL AWARDS 2026

RECRUITMENT OF SPECIALIST CADRE OFFICERS ON CONTRACT/ REGULAR BASIS (ADVERTISEMENT NO: CRPD/SCO/2026-27/11)

ONLINE REGISTRATION OF APPLICATION & PAYMENT OF FEES: FROM 07.08.2026 TO 27.08.2026

State Bank of India invites online applications from eligible Indian citizens for appointment to the Specialist Cadre Officers Posts on Contract/Regular Basis. Candidates are requested to apply online through the link given on Bank's official website https://sbi.bank.in/web/careers/current-openings. The candidates, who intend to apply for the Post(s) are advised to apply only after carefully reading and understanding the undernoted contents of this notification.

BRIEF SUMMARY OF THE ENGAGEMENT: POST: MUTIPLE POSTS (CUT-OFF DATE: 31.07.2026)

Posts	Age (in Years)	Educational Qualification	Experience
Deputy Vice President (DVP) – Cyber Innovation & Simulation Lab	**Min- 35 Max-45**	Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies.	Overall experience of 12+ years with at least 6 years in Technology Innovation/ IT Innovation/ Digital Innovation/ Emerging Technologies/ Cyber Security Innovation/ Technology Strategy/ Innovation Labs/ Centers of Excellence (CoE), Digital Transformation/ Product Innovation/ Technology Consulting or related domains.
Deputy Vice President (DVP) – Citizen Centric Initiatives			Minimum 12 years' experience in BFSI IT / Information Security /Cyber Security with at least 6 years in cyber security/ conducting cybersecurity awareness.
Deputy Vice President (DVP) – Cyber Security			Minimum 12 years' experience in BFSI IT/ Information Security / Cyber Security with at least 6 years in Cyber Research/Cyber Defence & Intelligence.
Deputy Manager- AI Specialist	**Min- 25 Max-35**	B. Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Data Science & Artificial Intelligence/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines with minimum 50% score. OR MCA OR M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Data Science & Artificial Intelligence/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines.	4 years post qualification experience in Information Technology domain. Out of 4 years, 2 years' experience in Designing ML/Deep Learning Models /mapping workflows/ deploying GenAI/RAG pipelines / Secure API Deployment / Experience with cloud ML suits like AWS SageMaker, Google Cloud Vertex AI or Microsoft Azure ML/ Expertise in libraries like TensorFlow, PyTorch, Scikit-Learn, Pandas/ XGBoost/ Hugging Face/ Lang Chain/ Open AI API / Apache Spark/Python/ Prompt Engineering/ Fine Tuning.
Deputy Manager- IT Security Expert	**Min- 25 Max-35**	B. Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines with minimum 50% score. OR MCA OR M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics &	Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain.

		Communications Engineering or Equivalent Degree in above specified disciplines.	
Deputy Manager - Cyber Security Analyst	**Min- 25** **Max-35**	B. Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines with minimum 50% score. OR MCA OR M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines.	Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain.

IMPORTANT INSTRUCTIONS:

1.	Before applying, candidates are requested to ensure that they fulfil the eligibility criteria for the post(s), as on the date of eligibility. Candidates are required to apply online through the website **https://sbi.bank.in/web/careers/current-openings** The process of Registration is completed only when fee is deposited with the Bank through online mode on or before the last date for payment of fee.
2.	Candidates are required to apply for the post(s) online through the link given on Bank's official website only and no other mode of application will be entertained. Hard copy of application & other documents need not to be sent to this office. Candidates are advised in their own interest to apply online well before the closing date and not to wait till the last date to avoid the possibility of disconnection / inability/ failure to log on to the website on account of heavy load on internet or website jam. SBI does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of aforesaid reasons or for any other reason beyond the control of SBI.
3.	Before submission of the application, candidates must check that they have filled in correct details in each respective field of the application form. After expiry of window for online application, no change/correction/modification will be allowed under any circumstances. Requests received in this regard in any form like Post, Email, by hand etc. shall not be entertained and will be summarily rejected.
4.	Candidates must have valid Email ID and Mobile phone number which should be kept active till the declaration of result and issuance of call letters on final selection, if any. It will help him/her in getting call letter/Interview advice etc. by email or over mobile by SMS.
5.	The Bank reserves the right to post / transfer the recruited / engaged officers to any of the offices of State Bank of India, in India or to depute to any of the associates / subsidiaries or any other organization depending upon the exigencies of the services. Request for posting / transfer to specific circle/place / office may not be entertained.
6.	Candidates are advised to check Bank's website **https://sbi.bank.in/web/careers/current-openings** regularly for details and updates. **No separate intimation will be issued in case of any change / update. All Changes/ Updates/ revisions / Corrigendum / results / schedules / list of shortlisted / selected candidates etc. will be hosted only on Bank's website only.** The Call letter/ advice, wherever required, will be sent by e-mail only **(No hard copy will be sent**).
7.	Candidates are required to upload all required documents (Resume, ID proof, Age proof, Caste Certificate (if applicable), PwBD Certificate (if applicable), Educational qualification, other qualifications/ certifications, Proof of Experience etc.) failing which their application / candidature will not be considered for Shortlisting / Interview.
8.	The Candidates applying for the post should ensure that their admission to all the stages of the recruitment (e.g. shortlisting, interview etc.) will be purely provisional subject to satisfying the prescribed eligibility conditions. Short listing will be provisional without verification of documents. Candidature will be subject to verification of all details/ documents with the original when a candidate reports for interview (if called).
9.	The selected candidates may be offered appointment in the bank subject to their completing other formalities such as verification of eligibility, credentials, certificates, satisfactory reports from the references, medical examination and verification of antecedents etc.
10.	Candidate(s) seeking age relaxation, fee exemption must submit valid requisite certificate of the Competent Authority in the prescribed format, when such certificate is sought at the time of document verification. Otherwise, their claim will not be entertained, and their candidature will be liable for cancellation / rejection.

11.	Candidates against whom there is/ are adverse report regarding character & antecedents, moral turpitude are not eligible to apply for the post. If any such adverse orders / reports against the shortlisted/ selected candidates is found/ received by the Bank post their selection, their candidature/ services will be rejected forthwith.
12.	**Candidates are not allowed to apply for more than One post.**
13.	In case more than one application (multiple applications) are submitted by a candidate for the **same post**, only the last valid (completed) application will be retained, and the application fee, if any, paid for the other registrations will stand forfeited. Further, multiple attendance/ appearance by a candidate at the time of interview / joining will result in rejection/ cancellation of candidature, summarily.
14.	**In case a candidate applies for more than One post, only the last valid (completed) application for two different posts will be retained, and the application fee, if any, paid for the other registrations will stand forfeited.**
15.	The Bank reserves the right to change the notified vacancies including the reserved vacancies without assigning any reason(s), whatsoever.
16.	The Bank reserves the right to cancel / modify the recruitment process entirely or partially at any stage / time for any particular post / all the posts, if so warranted, without assigning any reason thereof and the Bank shall not be liable to refund the fee or pay any compensation to the applicant.
17.	Candidates furnishing false information / suppressing the facts will be disqualified and shall be liable for debarment and legal/criminal action. Candidates who attempt fraud/impersonation shall be liable to be debarred from future recruitment process conducted by the Bank.
18.	The selected candidates, after appointment, shall be on probation as per Bank's extant recruitment Policy in force / amended/ modified from time to time, for the respective Post(s).
19.	All appointments under this project shall be entirely at the discretion of the Bank and shall be made at the starting stage of the pay scale admissible to the post.
20.	The Bank will decide the Venues(s) / Centre(s) for interview, if shortlisted. Candidates will have to appear for the interview, if called, at a center / venue as decided by the Bank and no request in this regard will be entertained by the Bank.
21.	In case a candidate is called for interview and is found not satisfying the eligibility criteria (Age, Educational Qualification, Other qualification, Experience etc.) he/ she will neither be allowed to appear for the interview nor be entitled for reimbursement of any travelling expenses.
22.	In case more than one candidate score same marks as cut-off marks in the final merit list (common marks at cut-off point), such candidates will be ranked in the merit according to their age in descending order.
23.	The Bank takes no responsibility for any delay in receipt or loss of any communication, whatsoever.
24.	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 will not be considered** and travelling expenses, if any, otherwise admissible, will not be paid.
25.	Candidates who applied in EWS Category, needs to submit the **EWS Certificate based on the income for FY. 2025-26, failing which their candidature will not be considered** and travelling expenses, if any, otherwise admissible, will not be paid.
26.	In case of selection, candidates will be required to produce proper discharge certificate from the current employer at the time of taking up the appointment.

A. DETAILS OF POSTS/ NATURE OF ENGAGEMENT /GRADE / VACANCY/ AGE:

Sl. No.	Name & Type of Post	Nature of Engagement/Grade	Vacancies						PwBD #	Age in years^ (As on 31.07.2026)	
			UR	SC	ST	OBC	EWS	Total	VI	Min	Max
1.	**Deputy Vice President (DVP) – Cyber Innovation & Simulation Lab**	**Contractual (SMGS-V)**	**1**	**--**	--	**--**	**--**	**1**	--	35	45
2.	**Deputy Vice President (DVP) – Citizen Centric Initiatives**		1	--	--	**--**	**--**	1	--		
3.	**Deputy Vice President (DVP) – Cyber Security**		2	--	--	**--**	**--**	2	1		
4.	**Deputy Manager- AI Specialists**	**Regular**	**12**	**4**	1	**6**	**2**	**25**	1	25	35
5.	**Deputy Manager- IT Security Expert**		**2**	**--**	**--**	**--**	**--**	**2**	1		
6.	**Deputy Manager - Cyber Security Analyst**		**2**	**--**	**--**	**1**	**--**	**3**	1 (Backlog)		
	Total		**22**	**4**	**1**	**7**	**2**	**34**	**4**		

- Horizontal vacancy
^ Age relaxation is available as per Government of India guidelines.

ABBREVIATIONS: **UR –** Unreserved, **OBC**-Other Backward Classes, **SC**-Scheduled Caste, **ST**-Scheduled Tribe, **EWS- Economically Weaker Section, PwBD** - Persons with Benchmark Disabilities, **VI**- Visually Impaired

IMPORTANT POINTS:

1. Reservation for PwBD candidates is horizontal and is included in the overall vacancy of the respective parent category (wherever applicable).
2. The number of vacancies including reserved vacancies mentioned above are **provisional and may vary** according to the actual requirement of the Bank.
3. Posting / Placement / Utilization of the selected candidates will be done at the sole discretion of the Bank.
4. Maximum age indicated is for Unreserved category candidates. **Relaxation in upper age limit** will be available to reserved category candidates as per Govt. of India guidelines (wherever applicable).
5. The reservation under various categories will be as per Government of India Guidelines (wherever applicable).
6. Candidate belonging to OBC category but coming in the 'Creamy Layer' are not entitled to OBC reservation and age relaxation. They should indicate their category as 'UR' or UR (PwBD) as applicable.
7. A declaration will have to be submitted in the prescribed format by candidates seeking reservation under OBC category stating that he/she does not belong to the creamy layer as on last date of online registration of application. **OBC certificate containing the 'non-creamy layer' clause, issued during the period 01.04.2026 to the date of interview, should be submitted by such candidates, if called for interview**. No request for extension of time for production of requisite certificate beyond the said date shall be entertained and candidature will be cancelled.
8. The EWS candidates are required to produce for verification the 'Income & Asset Certificate' **issued based on gross annual income for the Financial Year 2025-26 and valid for the year 2026-27 as per extant DoPT guidelines, on the date of document verification at the time of interview**. 'Income & Asset Certificate' issued based on gross annual income for the financial year 2025-26 must be obtained by the candidates on or before the date of document verification at the time of interview. **No request for extension of time for production of 'Income & Asset Certificate' beyond the said date** shall be entertained and if a candidate fails to produce the 'Income & Asset Certificate' at the time of interview, he/ she will not be allowed for interview and not considered for appointment in the Bank for the post.
9. Candidates belonging to reserved category including Person with Benchmark Disabilities (PwBD) for whom no reservation has been mentioned above, are free to apply for vacancies announced for Unreserved category provided they fulfil all the eligibility criteria applicable to Unreserved Category.
10. Benefit of reservation/ relaxation (**if any**) under reserved category (i.e. SC, ST, OBC) including PwBD category can be availed of only upon production of valid Caste certificate issued by the Competent Authority on format **prescribed by the Government of India.**

11. Relaxation in Upper age limit shall be as below (**wherever applicable**):

Sl.	Category		Age relaxation (In years)
a)	Other Backward Classes (OBC) (Non-Creamy Layer)		3
b)	Scheduled Castes/ Scheduled Tribes (SC/ ST)		5
c)	Persons with Benchmark Disabilities (PwBD)	- PwBD (UR/ EWS)	10
		- PwBD (OBC)	13
		- PwBD (SC/ ST)	15

NOTE: Cumulative age relaxation will not be available either under the above items or in combination with any other items. Candidates seeking age relaxation are required to submit copies of necessary certificate(s) at the time of interview, if shortlisted. No change in the category of any candidate is permitted after registration of online application, no correspondence/email/phone will be entertained in this regard.

12. PwBD candidate should produce a certificate issued by a competent authority as per the Government of India Guidelines (wherever applicable).

13. Only persons with **benchmark disabilities** would be eligible for reservation under PwBD category. "**Benchmark disability**" means a person with not less than 40% of a specified disability where specified disability has not been defined in measurable terms and includes the persons with disability, where disability has been defined in a measurable term, as certified by the certifying authority. A person who wants to avail the benefit of reservation will have to submit latest Disability Certificate, on prescribed format, issued by Medical Authority or any other notified Competent Authority (Certifying Authority). **The certificate should be dated on or before last date of registration of application. In absence of valid certificate, the candidature will be liable for cancellation / rejection and no communication in this regard will be entertained by the Bank.** Horizontal reservation has been provided to Persons with Benchmark Disabilities as per section 34 of "The Rights of Persons with Disabilities Act (RPWD), 2016". Suitable categories of disabilities and Functional requirements for the post(s) will be in reference to the Gazette of India, Notification No. 38-16/2020-DD-III dated 4th January 2021, Ministry of Social Justice and Empowerment [Department of Empowerment of Persons with Disabilities (Divyangjan)].

(B) Details of Educational Qualification/ Certification/ Work Experience/ Specific Skills Required:

Post No / Post Name	1 – DVP- Cyber Innovation & Simulation Lab
BASIC QUALIFICA **(AS ON 31.07.2026)**	**Mandatory:** Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies
OTHER CERTIFICATIONS **(AS ON 31.07.2026)**	**The preferred certifications**: CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management) **(Certification should be valid as on last date of registration.)**
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.07.2026)**	**Mandatory:** Overall experience of 12+ years with at least 6 years in Technology Innovation/ IT Innovation/ Digital Innovation/ Emerging Technologies/ Cyber Security Innovation/ Technology Strategy/ Innovation Labs/ Centers of Excellence (CoE), Digital Transformation/ Product Innovation/ Technology Consulting or related domains. **Preferred:** • Experience in working or managing a cyber–Security Innovation initiatives and Simulation of cyber solutions. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.

SPECIFIC SKILLS	• Strong leadership and management skills, with the ability to motivate and inspire a team. • Good technical knowledge of cybersecurity domains. • Training and dissemination of technical skills, identifying needs and owning skilling and sensitization programs. • Knowledge of Cyber Labs and Modern Learning technologies. • Excellent written and verbal communication skills, with the ability to explain complex technical concepts to diverse audiences. • Strong project management skills, with the ability to plan, organize, and execute complex training initiatives. • Ability to identify and solve complex problems related to cybersecurity training and education. Ability to adapt to changing technologies and industry trends. • Exposure to public private partnership models or Centre of Excellence • Deep understanding of BFSI Sectoral Cyber Security & risks.

Post No / Post Name	**2 – DVP- Cyber Citizen Centric Initiatives**
BASIC QUALIFICA **(AS ON 31.07.2026)**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology.
OTHER CERTIFICATIONS **(AS ON 31.07.2026)**	**Preferred certifications:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management) **(Certification should be valid as on last date of registration.)**
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.07.2026)**	**Mandatory:** Minimum 12 years' experience in BFSI IT / Information Security /Cyber Security with at least 6 years in cyber security/ conducting cybersecurity awareness. **Preferred:** • Experience in working or managing a cyber security-related citizen awareness activity like Cyber related mass and niche awareness programs through varied channels/ modes. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. **Training & Teaching experience will not be counted for eligibility.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Strong leadership and management skills. • Driving and owning citizen and end user security programs and gauging their effectiveness. • Creating metrics and tracking the development of a program for outreach and Cyber user safety. • Excellent communication and interpersonal skills. • Technical expertise in relevant areas like IT, cybersecurity, and data management. • Experience in project management and program delivery. • Knowledge of relevant policies, regulations, and best practices.

	• Ability to work effectively in a fast-paced environment. • Experience with stakeholder engagement and relationship management • Mentoring a team of professionals involved in citizen-centric initiatives

Post No / Post Name	3 – DVP- Cyber Security
BASIC QUALIFICATION (AS ON 31.07.2026)	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recogn by Govt. of India / approved by Govt. Regulatory bodies. OR MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies**.** **Preferred:** An advanced degree in Cybersecurity or Information Technology.
OTHER CERTIFICATIONS (AS ON 31.07.2026)	**Preferred certifications:** **CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)** **(Certification should be valid as on last date of registration.)**
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.07.2026)	**Mandatory:** Minimum 12 years' experience in BFSI IT/ Information Security / Cyber Security with at least 6 years in Cyber Research/Cyber Defence & Intelligence**.** **Preferred:** • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, Cyber Research or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence) **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Deep understanding of cybersecurity principles, technologies, and best practices. • Proven experience in leading research and thought leadership initiatives. • Experience in developing and implementing cybersecurity strategies. • Expertise in security technologies, including firewalls, intrusion detection/prevention systems, SIEM, and endpoint protection. • Proficiency in threat intelligence platforms and tools. • Knowledge of cyber forensics and incident response procedures • Analyzing the likelihood that an emerging threat will impact their organization and identify where weaknesses are. • Defining reports and recommendations to the business to enable the effectiveness of mitigation and remediation efforts. • Ability to develop and implement a comprehensive cybersecurity strategy. • Ability to analyze complex security issues and develop effective solutions. • Ability to assess, mitigate, and manage cyber security risks. • Experience in managing and responding to cyber security incidents. • Knowledge of relevant cybersecurity standards, regulations, and best practices.

Post No / Post Name	4 – Deputy Manager- AI Specialists
BASIC QUALIFICATION (AS ON 31.07.2026)	**Mandatory**: B. Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Data Science & Artificial Intelligence/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines with minimum 50% score. OR MCA OR M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Data Science & Artificial Intelligence/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines from a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies.
OTHER CERTIFICATIONS (AS ON 31.07.2026)	**Professional certifications:** 1. Advanced in AI Audit (AAIA) from ISACA USA 2. Advanced in AI Security Management (AAISM) from ISACA USA 3. Advanced in AI Risk (AAIR) from ISACA USA 4.AWS Certified AI Practitioner 5.Goolge Cloud Professional ML Engineer. 6.IBM AI Engineering Professional Certificate.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.07.2026)	**Mandatory: 4** years' post qualification experience in Information Technology domain. Out of 4 years, 2 years' experience in Designing ML/Deep Learning Models /mapping workflows/ deploying GenAI/RAG pipelines / Secure API Deployment / Experience with cloud ML suits like AWS SageMaker, Google Cloud Vertex AI or Microsoft Azure ML/ Expertise in libraries like TensorFlow, PyTorch, Scikit-Learn, Pandas/ XGBoost/ Hugging Face/ Lang Chain/ Open AI API / Apache Spark/Python/ Prompt Engineering/ Fine Tuning. **Preferred:** Experience in AI Related Domain would be Preferred **Training & Teaching experience will not be counted for eligibility.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• **Integration, Testing & Deployment**: Understand integration requirements, coordinate with internal tech teams, prepare test cases, validate data flow and system compatibility. Monitor and troubleshoot AI systems in real-time. • **AI/ML Development & Optimization**: Develop and implement AI algorithms and models including SLMs, LLMs, CNNs, GANs, agents, harnesses, guardrails. Analyze, preprocess large datasets. Evaluate model performance, fine-tune for optimal results. Optimize models through hardware and software design for data flow and inference. • **Data, Cloud & Infrastructure**: Work with big data technologies like Hadoop and Spark. Use cloud platforms such as AWS, Google Cloud, or Azure. Handle hardware requirements for training, fine tuning, and deployment. • **Security & Compliance**: Conduct security assessments of AI models using adversarial AI tools. Identify model poisoning, biases, and vulnerabilities. Ensure ethical considerations and compliance with relevant regulations. • **Research, Documentation & Collaboration**: Conduct research and maintain published track record in AI/ML. Develop and maintain documentation for AI models and solutions. Participate in code reviews and contribute to team knowledge sharing. Use version control systems like Git.

	• **Technical Skills & Awareness**: Proficiency in programming languages such as Python, Java, or C++. Experience with AIML frameworks and libraries. Stay current with industry trends and advancements in AI and machine learning.

Post No / Post Name	**5 – Deputy Manager- IT Security Expert**
BASIC QUALIFICATION **(AS ON 31.07.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines from a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies. **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.07.2026)**	**Preferred Certifications:** ISO 27001/ CISSP/ CISA/CRISC/CISM/CCSP/GDPR/ DPDPA/Advanced certifications or postgraduate diplomas in cybersecurity governance, risk and compliance..
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.07.2026)**	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** • Minimum 2 years of post-qualification experience in the Cyber Security Compliance roles. • Solid understanding of banking and financial industry regulation and compliance requirements like RBI's Cybersecurity Framework, SEBI's Cybersecurity Guidelines/ ISO 27001/ NIST/ SOC2/ PCI DSS/ GDPR/ DPDPA/India's NCIIPC/ CERT-In frameworks. • Understanding of BFSI sectoral Cybersecurity Risk and its mitigations. **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of job, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of job and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Good knowledge of cyber security regulations, standards, and frameworks (ISO 27001/ NIST/SOC2/PCI-DSS, etc.). • Experience in compliance monitoring, audit management, and policy governance. • Familiarity with IT General Controls (ITGC) and risk management frameworks. • Excellent written and verbal communication. • Ability to collaborate with cross-functional teams and external regulators. • Keeping abreast of changes in regulations and industry standards. • Strong understanding of relevant regulations and compliance frameworks. • Exceptional communication and interpersonal skills (written and verbal). • Ability to work independently and as part of a team. • Experience in risk management or a related field is an added advantage.

Post No / Post Name	**6 – Deputy Manager -Cyber Security Analyst**
BASIC QUALIFICATION **(AS ON 31.07.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies).

OTHER CERTIFICATIONS (AS ON 31.07.2026)	**Preferred Certifications:** ISO27001/CISSP/CISA/CRISC/CISM/CCSP/GDPR/ DPDPA/Advanced certifications or postgraduate diplomas in cybersecurity policy / compliance.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.07.2026)	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Minimum 2 years post-qualification experience in the IT Security policy / Cyber Security policy development, technical writing, or governance, risk & compliance (GRC) roles. Experience in documenting standards or frameworks like ISO 27001/ NIST/ SOC2/ PCI DSS/ GDPR/DPDPA/ India's NCIIPC/ CERT-In frameworks. Experience in Policy advocacy and dissemination domains. Excellent verbal and written communication skills. **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Strong analytical and research skills, with the capacity to interpret complex policies and trends. • Demonstrated ability to build and maintain relationships with key stakeholders and influence policy decisions. • Team player with strong collaboration and interpersonal skills. • Organized, methodical, and structured in thinking and writing. • Ability to present complex information clearly and concisely to diverse audiences. • This position requires a combination of technical expertise, policy knowledge, and skills to effectively advocate • Advocacy includes a range of activities such as public awareness campaigns, expert briefs, legislative lobbying, and engaging with policymakers to advocate for specific policy outcomes. • Hands on experience and skills to control vulnerability and deliver cyber centric policies and strategies adept with latest regulatory and technical of cyber security, to translate them effectively as a policy. • Creation and implementation of cyber policies. • Understanding of policy implementation process.

IMPORTANT POINTS:

1. The educational qualification prescribed for the post is minimum. Candidate must possess the Post Basic qualification and relevant full-time experience as on specified dates.
2. **The relevant experience certificate from the employer must contain specifically that the candidate had experience in that related field as required.**
3. In cases where the certificate of degree/diploma does not specify the field of specialization, the candidate will have to produce a certificate from the concerned university/college specifically mentioning the specialization.

C. DETAILS OF BRIEF JOB PROFILE, ROLE & RESPONSIBILITIES, FUNCTIONS & ACTIVITIES:

Sl	POST	Detail description of Job Profile, Role, Responsibilities, and Functions.
1.	**DVP- Cyber Innovation & Simulation Lab**	**Job Profile:** To lead the Innovation & Simulation Lab within the CoE, fostering a culture of experimentation, prototyping, and applied research. The role focuses on driving strategic innovation, simulating real world cybersecurity and technology challenges, and accelerating the development and testing of emerging solutions to future-proof the organization's digital and cyber capabilities. **KRAs:** **Key Responsibilities:** **Innovation Strategy:** • Define a comprehensive innovation strategy aligned with the CoE's goals and the organization's overall cybersecurity objectives. **Innovation Lab:** • Enable the design of innovation and research lab to ensure state-of-the-art facilities. • Establish framework for research and innovation activities including infrastructure enablement, operational models, outcome measurement etc. • Drive strategic and operational relationships for implementation and operations of the lab.

		Operational Excellence: • Ensure the lab operates efficiently, with effective resource allocation and project management practices. • Monitor and report on the progress of research initiatives and innovation projects. • Manage the lab's budget, ensuring optimal use of resources for maximum impact. **Innovation and Solution Development:** • Translate research findings into practical cybersecurity solutions and strategies. • Evaluate and integrate emerging technologies and methodologies into existing frameworks. • Promote the development of prototypes /toolkits and proof-of-concept demonstrations to showcase new technologies. **Emerging Technologies:** • Research and assess emerging cybersecurity technologies, such as AI, machine learning, blockchain, and quantum computing, to identify potential applications and opportunities for the CoE. **Knowledge Sharing:** • Foster a culture of knowledge sharing and collaboration within the CoE, facilitating the dissemination of best practices, research findings, and lessons learned. **External Engagement:** • Build and maintain relationships with external stakeholders, including industry experts, research institutions, and technology vendors, to stay abreast of the latest trends and foster collaboration. **Talent Development:** • Identify and nurture talent within the CoE, providing opportunities for professional development and growth in areas related to innovation and cybersecurity. **Performance Measurement:** • Define and track key performance indicators (KPIs) to measure the effectiveness of innovation initiatives and the overall impact of the CoE. **Security Posture Enhancement:** Continuously improve the organization's security posture through the adoption of innovative solutions and best practices.
2.	**DVP- Cyber Citizen Centric Initiatives**	**Job Profile:** To lead, design, and implement citizen-centric initiatives aligned with organizational goals, ensuring services are accessible, inclusive, efficient, and impactful. The role demands strategic thinking, strong stakeholder engagement, program management capabilities, and a deep understanding of citizen needs in digital and physical governance initiatives. Formulate and lead the vision and roadmap for citizen-centric programs under the CoE. **KRAs:** ➢ Developing and Implementing Cybersecurity Strategies: • This includes creating and executing plans to protect citizens from cyber threats, such as cybercrime, online fraud, and data breaches. ➢ Program Management: • Overseeing the planning, execution, and delivery of citizen centric projects, ensuring they are completed on time and within budget. • Coordinating across different departments and teams to ensure seamless integration and implementation of initiatives. • Monitoring project progress, identifying potential risks and issues, and implementing mitigation strategies. ➢ Promoting Cyber Awareness and Literacy: • Educating citizens about online safety, digital citizenship, and responsible online behavior is crucial. ➢ Ensuring Access to Secure Digital Services: • Working to make government services accessible and secure for all citizens, regardless of their technical expertise. ➢ Fostering Collaboration:

		• Working with various stakeholders, including law enforcement, technology companies, and non-profit organizations, to create a safer online environment. ➢ Leading a Team: • Managing and mentoring a team of cybersecurity professionals to achieve the initiative's goals. ➢ Technical Expertise: • Providing technical guidance and support for the design and implementation of citizen-centric solutions. • Staying up-to-date on emerging technologies and trends in areas like IoT, smart infrastructure, cybersecurity, and e governance. • Evaluating and recommending appropriate technologies for specific citizen-facing applications.
3.	**DVP- Cyber Security**	**Job Profile:** This role involves leading research initiatives, developing thought leadership content, and fostering a culture of cybersecurity excellence within the organization and externally. The role oversees and manages the cyber security strategy and operations for an organization, focusing on threat detection, incident response, and intelligence gathering. This includes building and managing a team, developing and implementing security policies and procedures, conducting threat intelligence analysis, and responding to cyber incidents. They are responsible for shaping the organization's perspective on emerging cybersecurity threats and best practices, and for contributing to the broader cybersecurity discourse. **KRAs:** ➢ Strategic Planning: • Define and enhance the global cyber defence & intelligence Program. • Develop and execute the CoE's cyber defense and intelligence strategy, aligning it with the organization's overall business objectives. ➢ Threat Intelligence & Cyber Defence: • Ensuring effective threat detection, incident response, and vulnerability management. • Communicating effectively with senior management, business units, and other stakeholders regarding cyber security risks, incidents, and mitigation plans. • Monitor, analyze, and disseminate threat intelligence from various sources to identify emerging threats and vulnerabilities. • Conduct forensic investigations of cyber incidents to identify the root cause and attacker methods. ➢ Cyber Defense: • Advanced Malware and forensics skills • Design and Implement and Malware and Forensics Lab ➢ Security Architecture: • Design, implement, and maintain robust security architectures and systems to protect the organization's digital assets. ➢ Threat Detection and Prevention: • Proactively monitor the environment for potential threats, using various tools and techniques, and implement preventative measures. ➢ Incident Response: Define and maintain incident response plans and procedures and lead the response to cyber security incidents. ➢ Developing and Implementing Cybersecurity Strategies: • This includes creating and executing plans to protect citizens from cyber threats, such as cybercrime, online fraud, and data breaches.

		➢ Program Management: • Overseeing the planning, execution, and delivery of citizen centric projects, ensuring they are completed on time and within budget. • Coordinating across different departments and teams to ensure seamless integration and implementation of initiatives. • Monitoring project progress, identifying potential risks and issues, and implementing mitigation strategies. ➢ Promoting Cyber Awareness and Literacy: • Educating citizens about online safety, digital citizenship, and responsible online behavior is crucial. ➢ Ensuring Access to Secure Digital Services: • Working to make government services accessible and secure for all citizens, regardless of their technical expertise. ➢ Fostering Collaboration: • Working with various stakeholders, including law enforcement, technology companies, and non-profit organizations, to create a safer online environment.
4.	**Deputy Manager- AI Specialists**	**Job Profile:** 1. AI/ML Development & Integration: Support integration testing of AI/analytics models, dashboards, PoCs, and autonomous tools like LLM agents. Train SLMs, GANs, etc., and prep datasets for workflow automation. 2. AI Security Controls & Governance: Define security controls for AI dev, testing, deployment, and ops. Establish model integrity, authenticity, versioning, provenance controls, and KRIs/KPIs. Map controls to enterprise frameworks and ensure regulatory compliance. 3. Risk & Threat Assessment: Assess risks of foundation models, open source models, 3rd-party AI services, and hosting/inference infra. Conduct AI red teaming, adversarial testing, and RCA for AI security incidents. 4. Data Privacy & Protection: Secure sensitive/regulated data in AI systems. Evaluate anonymization, tokenization, masking, and privacy enhancing tech. Review AI solutions for privacy/confidentiality risks. 5. Infrastructure & Workload Security: Secure AI workloads on containers, Kubernetes, GPUs, and cloud-native platforms. Evaluate model hosting environments and serving infrastructure. 6. Governance, Reporting & Stakeholder Engagement: Present AI risks to senior management, participate in AI governance committees and architecture boards. Develop dashboards, support audits, and track emerging AI/ML threats. 7. Procurement, Supply Chain & Adoption: Support procurement/onboarding reviews for AI products. Review open-source AI components and supply chain risks. Establish secure GenAI usage guidelines for employees. **KRAs:** 1. AI/ML Development & MLOps: Train, fine-tune, and deploy SLMs, LLMs, CNNs, GANs for workflow automation. Build RAG pipelines, embeddings, and data repositories. Operationalize models using CI/CD, versioning, monitoring, retraining, and optimize for performance/cost. 2. Agentic Systems & Integration: Design autonomous LLM agents/harnesses that orchestrate end-to-end workflows. Support integration testing of AI models, dashboards, PoCs, and ensure compatibility with existing systems, APIs, plugins, and 3rd-party integrations. 3. AI Security Governance & Frameworks: Develop and implement organization-wide AI/LLM security governance framework and secure development standards. Establish controls for model integrity, authenticity, versioning, provenance across dev, testing, deployment, and ops. 4. Risk Assessment & Threat Modeling: Assess risks for foundation models, open-source models, 3rd-party AI services, and workloads on containers/Kubernetes/GPUs/cloud. Perform threat modeling for prompt injection, jailbreak, model poisoning, data leakage. Conduct adversarial testing and red teaming. 5. Data Privacy, Compliance & Guardrails: Safeguard sensitive/regulated data via anonymization, tokenization, masking, PHE tech. Secure RAG pipelines, vector DBs, and knowledge repos. Implement AI guardrails, content filtering, misuse prevention. Ensure alignment with RBI, CERT-In, DPDP Act, ISO 42001, NIST AI RMF, and other regulations. **6.** Monitoring, Incident Response & Stakeholder Engagement: Monitor AI apps for anomalies, abuse, and security incidents. Drive misuse/abuse detection, RCA, maintain AI asset inventory and risk register.

		Support incident response/forensics, audits, and present risks to senior management. Build AI security awareness and collaborate with infra, data, legal, compliance, and architecture teams.
5.	**Deputy Manager - IT Security Expert**	**Job Profile:** The IT Security Expert will be responsible for ensuring that the Cyber Security Centre of Excellence (CSCoE) adheres to internal policies, industry regulations, and applicable cyber security standards. The role involves monitoring compliance frameworks, performing risk assessments, developing and implementing policies, and coordinating with internal and external auditors to strengthen the organization's security posture. Cybersecurity Compliance Specialist will develop, review, and maintain comprehensive cybersecurity compliance dashboard for public sector and enterprise environments. **KRAs:** **Developing and Implementing Compliance Programs**: Creating and maintaining policies, procedures, and training materials related to compliance. **Conducting Audits and Assessments:** Regularly reviewing processes, practices, and documents to identify potential violations and areas of risk. **Monitoring Compliance:** Tracking adherence to regulations and internal controls, using compliance management platforms where appropriate. **Compliance Metrics**: Define and design Compliance metrics to assess how well an organization is adhering to standards. **Reporting**: Preparing and submitting compliance reports to regulatory bodies and internal stakeholders. **Risk & Audit Management** • Conduct compliance risk assessments and identify gaps in cyber security practices. • Coordinate with internal/external auditors during cyber security audits. • Track and remediate compliance findings, audit observations, and vulnerabilities. • Knowledge of regulatory environments (especially in IT Security, Cybersecurity and related Innovation areas). • Ability to identify and solve complex problems related to cybersecurity training and education. • Collaborate with stakeholders to understand various compliance requirements and produce compliance metrics for leadership team. • Understanding of advance cybersecurity concepts and latest technical advancement and disruptions • Create, review and managing metrics for Cyber Policies and Trainings. • Staying up to date on the latest cybersecurity threats, technologies and best practices in ever-evolving cybersecurity landscape.
6.	**Deputy Manager - Cyber Security Analyst**	**Job Profile:** Cybersecurity Analyst will develop, review, and maintain comprehensive cybersecurity policies, procedures, and compliance documentation for public sector and enterprise environments. The Analyst will be a strategic thinker and adept at translating and evidence into actionable policy change. Analyze data and provides evidence based recommendations to inform the development of policies. The role requires the ability to synthesize complex issues and present clear, actionable insights to stakeholders. Research, drafting, and advocacy initiatives. Track regulatory changes, policy papers, and government consultations relevant to Information Security & Cybersecurity. Prepare briefs, position papers, and analytical reports. Provide policy insights for decision-making and strategy development. Coordinate knowledge-sharing sessions with the Academy program team related to policy. They research emerging digital security issues, draft policy documents, collaborate with technical and non-technical teams, and ensure compliance with relevant regulations and frameworks. Their work involves bridging the gap between technical realities and policy requirements, translating complex cybersecurity concepts into clear guidelines for various audiences. **KRAs:** **On Ground Execution:** • In collaboration with the executive team, design and implement a comprehensive, multi-year advocacy strategy that aligns with the center's mission and goals. • Monitor and analyze legislative and regulatory developments at the local, state and national levels, providing strategic guidance to the organizations. • Ensure the center's advocacy work is informed and responsive to the needs of the communities we serve.

		Policy Development and Advocacy: • Oversee the development of high-quality, evidence-based policy materials, including reports, briefs, factsheets, and testimony. • Design and execute advocacy strategies to influence policy decisions at national, state and local level. • Engage with government bodies, regulators, industry associations and civil society stakeholders. • Represent the CSCoE in consultations, forums and working groups. • Develop and implement a comprehensive engagement strategy with government officials, regulators, and policymakers at the central, state, and local levels. • Identify and analyze emerging cybersecurity policies and regulations at national and international levels. • Represent the CSCoE in policy discussions and forums, advocating for the organization's positions and priorities. • Influencing policy frameworks, involves making submissions and recommendations to government bodies on complex issues like data protection, internet safety, and digital economy regulations. **Risk Assessment and Management**: • Identify and assess potential policy risks and opportunities for the CSCoE. • Develop and implement strategies to mitigate policy risks and capitalize on opportunities. • Implement & Monitor policy developments and provide timely updates to the CSCoE leadership. **Internal Collaboration**: • Work closely with other teams within the CSCoE, including research, technical, and training teams, to ensure alignment on policy matters. • Share knowledge and expertise with other teams to promote a common understanding of cybersecurity policy. **Reporting and Communication**: • Prepare reports and briefings on policy advocacy activities and outcomes. • Communicate policy developments and their potential impact to internal and external stakeholders. • The role focuses on translating complex regulations into actionable documents. • Demonstrate expertise in policy writing, risk assessments and government-aligned standards. • Collaborate with stakeholders to understand various requirements and produce technical documentation. • He / She will design training curriculum and create training materials accordingly. • Staying up to date on the latest cybersecurity threats, technologies and best practices in ever-evolving cybersecurity landscape. **Policy Research & Analysis**: • Conduct in depth research on policies, regulations to the organization or sector. • Analyze existing policies to identify gaps, inefficiencies and areas for improvement. • Stay up to date with cyber security, political, economic and social trends that may influence policy. **Develop Policy Recommendations**: • Develop clear, evidence-based policy recommendations based on research findings. • Researching, analyzing, and drafting new cybersecurity policies and standards related to areas like ransomware, incident response, and vulnerability management. • Provide actionable, practical suggestions to senior leadership or stakeholders for policy adjustments or new policy initiatives. • Policy research reports and briefing notes delivered on time. • High-quality inputs to advocacy papers, regulatory responses. **Policy Monitoring & Evaluation**: • Monitoring the implementation of policies to assess their effectiveness and impact. • Evaluate and assess the outcomes of policies and make adjustments as necessary. • Report on the progress of policies and recommend improvements based on real world data. • Prepare reports, dashboards, and presentations for leadership and policymakers. • Ensuring the cybersecurity policies adhere to legal requirements and industry frameworks, such as NIST. **Communicate findings**: • Prepare clear and concise reports and presentations to communicate policy analysis and recommendations. • Represent the organization in policy discussions, conferences and working groups. • Translating complex cybersecurity concepts into accessible language for both technical and non-technical audiences. **Support Strategic Initiatives**: • Support the creation of long – term policy strategies aligned with organization’s goals and values. • Contribute to the development of strategic frameworks for policy change.

Remarks: Actual KRAs shall be assigned on joining. Roles / Responsibilities / Job Profile mentioned above are illustrative. Roles / Responsibilities / Activities / Key Interactions/ Jobs in addition to the above mentioned may be assigned by the Bank from time to time depending upon the requirement.

The candidates selected for Regular posts will be governed by the Service Rules applicable to the employees of the SBI.

(D) REMUNERATION /SUGGESTED PLACE OF POSTING:

<table>
<tr><th>Sl. No.</th><th>Name of Post</th><th>Annual CTC Upper Range^
Rs. In Lakhs</th><th>Bifurcation of Annual CTC</th><th>Contract Period $</th><th>Place of Posting</th></tr>
<tr><td>1.</td><td>DVP- Cyber Innovation & Simulation Lab</td><td rowspan="3">Upper range - Rs. 60.00 Lacs</td><td rowspan="3"><table><tr><td>Fixed Pay</td><td>90% of CTC</td></tr><tr><td>Variable Pay#</td><td>10% of CTC</td></tr><tr><td>Annual Increment Band^^</td><td>Upto 10%</td></tr></table></td><td rowspan="3">3 Years. May be renewed for further period of 02 years at the discretion of Bank at mutually agreed terms and conditions (Total engagement period should not exceed 05 years).</td><td rowspan="6">Mumbai or anywhere in India, in case of any administrative requirement.</td></tr>
<tr><td>2.</td><td>DVP- Cyber Citizen Centric Initiatives</td></tr>
<tr><td>3.</td><td>DVP- Cyber Security</td></tr>
<tr><td>4.</td><td>Deputy Manager- AI Specialists</td><td colspan="2" rowspan="3">Basic: 64820-2340/1-67160-2680/10-93960

(The official will be eligible for DA, HRA, CCA, PF, Contributory Pension Fund i.e., NPS, LFC, Medical Facility, leave etc. as per rules in force from time to time and Salary and perks as per Bank’s salary structure)</td><td rowspan="3">REGULAR POST</td></tr>
<tr><td>5.</td><td>Deputy Manager- IT Security Expert</td></tr>
<tr><td>6.</td><td>Deputy Manager -Cyber Security Analyst</td></tr>
</table>

^ Annual CTC is negotiable and will depend upon experience & current emoluments of candidates in the present employment & place of posting.
$ The contract can be terminated at any time, without prejudice, by giving 3 Months’ notice from either side or on payment/surrender of 3 Months' compensation amount in lieu thereof.
^^ Annual increment if any proposed second year onwards upto 10% (Depending on performance)
 # The variable pay structure, depending on the performance of the contractual officer will be as under:

99 to 100%	100%
97 to 98.99 %	90%
94 to 96.99%	80%
90 to 93.99%	70%
Below 90%	Nil

E. <u>SELECTION PROCESS</u>: The selection will be on the basis of **Shortlisting and Interview.**

- **Shortlisting**: **Mere fulfilling the minimum qualification and experience will not vest any right to candidate for being called for interview.** The shortlisting committee constituted by the Bank will decide the shortlisting parameters and thereafter, adequate number of candidates, as decided by the Bank, will be shortlisted for interview. The decision of the Bank to call the candidates for the interview shall be final. No correspondence will be entertained in this regard.
- **Interview:** Interview will carry 100 marks. The qualifying marks in interview will be decided by the Bank. No correspondence will be entertained in this regard.
- **Merit List:** Merit list for selection will be prepared in descending order based on scores obtained in interview only. In case more than one candidate score the cut-off marks (common marks at cut-off point), such candidates will be ranked according to their age in descending order, in the merit list.

F. <u>CALL LETTER FOR INTERVIEW:</u> Intimation/call letter for interview will be uploaded on bank's website or sent by email, as decided by the Bank. **NO HARD COPY WILL BE SENT.**

G. HOW TO APPLY: Candidates should have **valid Email ID** which should be kept active till the declaration of result. It will help him/her in getting call letter/ **i**nterview advice etc. by email.

GUIDELINES FOR FILLING ONLINE APPLICATION	GUIDELINES FOR PAYMENT OF FEES
i. Candidates will be required to register themselves online through the link available on SBI website **https://sbi.bank.in/web/careers/current-openings** and pay the application fee using Internet Banking/ Debit Card/ Credit Card/ UPI etc. ii. Candidates should first scan their latest photograph and signature. Online application will not be registered unless candidate uploads his/ her photo and signature as specified on the online registration page (under 'How to Upload Document"). iii. Candidates should fill the application carefully. Once application is filled-in completely, candidate should submit the same. In the event of candidate not being able to fill the application in one go, he can save the information already entered. When the information/ application is saved, a provisional registration number and password is generated by the system and displayed on the screen. **Candidate should note down the registration number and password.** They can re-open the saved application using registration number and password and edit the particulars, if needed. This facility for editing the saved information will be available for three times only. Once the application is completely filled, candidate should submit the same and proceed for online payment of fee. iv. **After registering online, the candidates are advised to take a printout of the system generated online application form.** v. Candidates seeking Age relaxation are required to submit copies of necessary certificates at the time of document verification. No change in category of any candidate is permitted after registration of online application.	i. Application fees and Intimation Charges (Non-refundable) is ₹ 750/- (₹Seven Hundred Fifty only) for General/EWS/OBC candidates and no fees/intimation charges for SC/ ST /PwBD candidates. ii. After ensuring correctness of the particulars in the application form, candidates are required to pay the fees through payment gateway integrated with the application. No change/ edit in the application will be allowed thereafter. iii. Fee payment will have to be made online through payment gateway available thereat. The payment can be made by using Debit Card/ Credit Card/ Internet Banking/ UPI etc. by providing information as asked on the screen. Transaction charges for online payment, if any, will be borne by the candidates. iv. On successful completion of the transaction, e-receipt and application form, bearing the date of submission by the candidate, will be generated which should be printed and retained by the candidate. v. If the online payment of fee is not successfully completed in first instance, please make fresh attempts to make online payment. vi. A provision is there to reprint the e-Receipt and Application form containing fee details, at later stage. vii. **Application Fee once paid will NOT be refunded on any account NOR can it be adjusted for any other examination or selection in future.**

H. HOW TO UPLOAD DOCUMENTS:

a. Details of Document to be uploaded:	d. Document file type/ size:
i. Recent Photograph ii. Signature iii. Biodata (Format Attached) (PDF) iv. Resume (PDF) v. ID Proof (PDF) vi. Proof of Date of Birth (PDF) vii. Educational Certificates: Relevant Mark-Sheets/ Degree Certificate (PDF) viii. Experience certificates (PDF) ix. Caste Certificate / EWS Certificate (if applicable) (PDF) x. PwBD Certificate (if applicable) (PDF) xi. Preferred qualification / Certification (if any) (PDF) xii. Form-16/Offer Letter/Latest Salary slip from current employer (PDF) xiii. CTC Negotiation for contractual posts.	i. All Documents must be in PDF (except Photograph & Signature) ii. Page size of the document to be A4 iii. Size of the file should not be exceeding 500 kb. iv. In case of Document being scanned, please ensure it is saved as PDF and size not more than 500 kb as PDF. If the size of the file is more than 500 kb, then adjust the setting of the scanner such as the DPI resolution, no. of colors etc., during the process of scanning. Please ensure that Documents uploaded are clear and readable.

b. Photograph file type/ size:

i. Photograph must be a recent passport style colour picture.
ii. Size of file should be between 20 kb - 50 kb and Dimensions 200 x 230 pixels (preferred)
iii. Make sure that the picture is in colour, taken against a light-coloured, preferably white, background.
iv. Look straight at the camera with a relaxed face
v. 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
vi. If you have to use flash, ensure there's no "red-eye"
vii. If you wear glasses make sure that there are no reflections, and your eyes can be clearly seen.
viii. Caps, hats and dark glasses are not acceptable. Religious headwear is allowed but it must not cover your face.
ix. 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, no. of colour etc., during the process of scanning.

c. Signature file type/ size:

i. The applicant has to sign on white paper with Black Ink pen.
ii. The signature must be signed only by the applicant and not by any other person.
iii. The signature will be used to put on the Call Letter and wherever necessary.
iv. Size of file should be between 10 kb - 20 kb and Dimensions 140 x 60 pixels (preferred).
v. Ensure that the size of the scanned image is not more than 20 kb.
vi. **Signature in CAPITAL LETTERS shall NOT be accepted**.

e. Guidelines for scanning of photograph/ signature/ documents:

i. Set the scanner resolution to a minimum of 200 dpi (dots per inch)
ii. Set Color to True Color
iii. Crop the image in the scanner to the edge of the photograph/ signature, then use the upload editor to crop the image to the final size (as specified above).
iv. The photo/ signature file should be JPG or JPEG format (i.e. file name should appear as: image01.jpg or image01.jpeg).
v. Image dimensions can be checked by listing the folder/ files or moving the mouse over the file image icon.
vi. Candidates using MS Windows/ MSOffice can easily obtain photo and signature in .jpeg format not exceeding 50 kb & 20 kb respectively by using MS Paint or MSOffice Picture Manager. Scanned photograph and signature in any format can be saved in .jpg format by using 'Save As' option in the File menu. The file size can be reduced below 50 kb (photograph) & 20 kb (signature) by using crop and then resize option (Please see point (i) & (ii) above for the pixel size) in the 'Image' menu. Similar options are available in another photo editor also.
vii. While filling in the Online Application Form the candidate will be provided with a link to upload his/her photograph and signature.

f. Procedure for Uploading Document:

i. There will be separate links for uploading each document.
ii. Click on the respective link "Upload"
iii. Browse & select the location where the JPG or JEPG, PDF etc. file has been saved.
iv. Select the file by clicking on it and click the 'Upload' button.
v. Click Preview to confirm the document is uploaded and accessible properly before submitting the application. If the file size and format are not as prescribed, an error message will be displayed
vi. Once uploaded/ submitted, the Documents uploaded cannot be edited/ changed.
vii. **After uploading the photograph/ signature in the online application form candidates should check that the images are clear and have been uploaded correctly.** In case the photograph or signature is not prominently visible, the candidate may edit his/ her application and re-upload his/ her photograph or signature, prior to submitting the form. **If the face in the photograph or signature is unclear the candidate's application may be rejected.**

I. GENERAL INFORMATION:

I. Before applying for the post, the applicant should ensure that he/ she fulfils the eligibility and other norms mentioned above for that post as on the specified date and that the particulars furnished by him/ her are correct in all respects.

II. Candidates belonging to reserved category including, for whom no reservation has been mentioned, are free to apply for vacancies announced for General category provided they must fulfil all the eligibility conditions applicable to General category.

III. **In case it is detected at any stage of recruitment that an applicant does not fulfil the eligibility norms and/ or that he/ she has furnished any incorrect/ false information or has suppressed any material fact(s), his/ her candidature will stand cancelled. If any of these shortcomings is/ are detected even after appointment / final selection, his/ her services/contracts are/ is liable to be terminated forthwith.**

IV. The applicant should ensure that the application is strictly in accordance with the prescribed format and is properly filled.

V. Engagement/Appointment of selected candidate is subject to his/ her being declared medically fit as per the requirement of the Bank. Such engagement/appointment will also be subject to the service and conduct rules of the Bank for such post in the Bank, in force at the time of joining the Bank.

VI. Candidates are advised to keep their e-mail ID active for receiving communication viz. call letters/ Interview date advice etc., as no communication may be sent in hard copy.

VII. The Bank takes no responsibility for any delay in receipt or loss of any communication whatsoever.

VIII. 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 shall not be considered and travelling expenses, if any, otherwise admissible, will not be paid.

IX. In case of selection, candidates will be required to produce proper discharge certificate from the employer at the time of taking up the engagement/appointment.

X. Candidates are advised in their own interest to apply online well before the closing date and not to wait till the last date to avoid the possibility of disconnection / inability/ failure to log on to the website on account of heavy load on internet or website jam. SBI does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of aforesaid reasons or for any other reason beyond the control of SBI.

XI. DECISION OF BANK IN ALL MATTERS REGARDING ELIGIBILITY, CONDUCT OF INTERVIEW, OTHER TESTS AND SELECTION WOULD BE FINAL AND BINDING ON ALL CANDIDATES. NO REPRESENTATION OR CORRESPONDENCE WILL BE ENTERTAINED BY THE BANK IN THIS REGARD.

XII. The applicant shall be liable for civil/ criminal consequences in case the information submitted in his/ her application are found to be false at a later stage.

XIII. Merely satisfying the eligibility norms does not entitle a candidate to be called for interview. Bank reserves the right to call only the requisite number of candidates for the interview after preliminary screening/ short-listing with reference to candidate's qualification, suitability, experience etc.

XIV. In case of multiple application, only the last valid (completed) application will be retained, the application fee/ intimation charge paid for other registration will stand forfeited.

XV. 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 alone shall have sole and exclusive jurisdiction to try and entertain any cause/ dispute.

XVI. Outstation candidates, who may be called for interview after short-listing will be reimbursed the cost of travelling by Air fare (Economy Class) for the shortest route in India, as given below

Post	Reimbursement Limit
(i) Deputy Manager- AI Specialists (ii) Deputy Manager- IT Security Expert (iii) Deputy Manager- Cyber Security Analyst	Reimbursement of Air Fare up to Rs. 10,000 (Total for both sides) or actual fare whichever is lower.
(i) DVP- Cyber Innovation & Simulation Lab (ii) DVP- Cyber Citizen Centric Initiatives (iii) DVP- Cyber Security	Reimbursement of Air Fare upto Rs. 15,000 (Total for both sides) or actual fare whichever is lower.

XVII. Request for change / correction in any particulars (including category in the application form, once submitted will not be entertained under any circumstances. No correspondence/phone/email will be entertained in this regard. Candidates are advised to fill up the online application carefully and furnish the correct information in this application.

XVIII. **BANK RESERVES RIGHT TO CANCEL / MODIFY THE RECRUITMENT PROCESS EITHER ENTIRELY OR PARTIALLY AT ANY STAGE / TIME FOR ANY PARTICULAR POST / ALL THE POST WITHOUT ASSIGNING ANY REASONS THEREOF, WHATSOEVER.**

XIX. **At the time of interview, the candidate will be required to provide details regarding criminal cases pending against him/her, if any.**
Suppression of material facts will result in cancellation/ termination of candidature at any point, even if the candidate is selected, his/her selection will be canceled in such circumstances. The Bank may also conduct independent verification, inter alia, including verification of Police Records, etc. The Bank reserves the right to deny the engagement/appointment depending upon such disclosure and/or independent verification.

DISCLAIMER (DPDP Act 2023)

xx. By applying to this position, you voluntarily provide your free, informed and unconditional consent for the collection and processing of your personal data by the Bank and sharing of such personal data with Data Processors as are required for the engagement process, in accordance with Digital Personal Data Protection Act, 2023 and the Rules made thereunder (collectively, the Act). The Bank has implemented all reasonable security safeguards to prevent breach of personal data in its possession or under its control, and your personal data will be handled with confidentiality and used solely for evaluating and verifying your eligibility, credentials, and candidacy for the advertised position and for certain legitimate uses as are permitted under the Act.

For any query, please write to us through link "CONTACT US/ Post Your Query" which is available on Bank's website (https://sbi.bank.in/web/careers/post-your-query)
The Bank is not liable for printing errors, if any.

State bank of India does not endorse, authorize or associate with any external coaching platform, consultancy, individual or digital channel claiming to provide guaranteed selection, influence in recruitment or insider guidance. Candidates must rely solely in information available on SBI's official career portal.

Mumbai
07.08.2026

GENERAL MANAGER (RP&PM)

HOW TO APPLY

Login to https://sbi.bank.in/web/careers/current-openings

Scroll down and click on the respective advertisement.

Download advertisement no. CRPD/SCO/2026-27/11
(Carefully read the detailed advertisement)

Apply Online
(Before final submission, please go through your application.
Corrections will not be allowed after final submission)