भारतीय स्टेट बैंक

केंद्रीय भर्ती एवं पदोन्नति विभाग, कॉर्पोरेट केंद्र, मुंबई
ईमेल: crpd@sbi.co.in

ग्लोबल फाइनेंस द्वारा एसबीआई को ''विश्व का सर्वश्रेष्ठ उपभोक्ता बैंक-2025'' और ''भारत का सर्वश्रेष्ठ बैंक-2025'' के रूप में मान्यता दी गई है.

नियमित आधार पर विशेषज्ञ संवर्ग के अधिकारियों की भर्ती

(विज्ञापन सं.: CRPD/SCO/2025-26/25)

आवेदन का ऑनलाइन पंजीकरण और शुल्क का भुगतान: दिनांक 24.02.2026 से 16.03.2026 तक

भारतीय स्टेट बैंक नियमित आधार पर विशेषज्ञ संवर्ग के निम्नलिखित पद पर नियुक्ति के लिए पात्र भारतीय नागरिकों से ऑनलाइन आवेदन आमंत्रित करता है. उम्मीदवारों से अनुरोध है कि वे बैंक की अधिकारिक वेबसाइट https://sbi.bank.in/web/careers/current-openings में दिए गए लिंक के माध्यम से ऑनलाइन आवेदन करें. इन पदों के लिए आवेदन करने के इच्छुक उम्मीदवारों को सूचित किया जाता है कि वे इस अधिसूचना की निम्नलिखित विषय-वस्तु को ध्यान से पढ़ने और समझने के बाद ही आवेदन करें.

महत्वपूर्ण सूचनाएँ:

1. उम्मीदवारों से अनुरोध है कि वे आवेदन करने से पहले, यह सुनिश्चित करें कि वे पात्रता की तिथि पर उक्त पद के लिए दिए गए योग्यता मानदंडों को पूरा करते हों. उम्मीदवारों को वेबसाइट **https://sbi.bank.in/web/careers/current-openings** का उपयोग करके ऑनलाइन आवेदन करना होगा. पंजीकरण की प्रकिया तभी पूरी होगी जब बैंक में ऑनलाइन माध्यम से शुल्क भुगतान की अंतिम तिथि या उससे पहले शुल्क जमा करवा दिया गया हो.
2. उम्मीदवारों को बैंक की आधिकारिक वेबसाइट पर दिए गए लिंक के माध्यम से ही ऑनलाइन आवेदन करना होगा तथा आवेदन का कोई अन्य तरीका स्वीकार नहीं किया जाएगा. इस कार्यालय को आवेदन एवं अन्य दस्तावेजों की कागजी प्रतियाँ न भेजें. उम्मीदवारों को उन्हीं के हित के लिए यह सूचना दी जाती है कि वे अंतिम तारीख से पहले समय रहते ही ऑनलाइन आवेदन प्रस्तुत कर दें और वे अंतिम तारीख का इंतज़ार न करते रहें क्योंकि बाद में हो सकता है कि वेबसाइट को लॉग ऑन करने में डिसकनेक्शन/अक्षमता/फेलियर की स्थिति बन जाए इन्टरनेट पर भारी लोड या फिर वेबसाइट जाम होने के कारण ऐसा हो जाए. यदि पूर्वोक्त कारणों से या एसबीआई के नियंत्रण से बाहर के किसी भी कारण से यदि उम्मीदवार अपना आवेदन समय रहते नहीं कर पाते हैं, तो इसके लिए एसबीआई किसी भी तरह से जिम्मेदार नहीं होगा.
3. आवेदन प्रस्तुत करने से पहले, उम्मीदवारों को यह जांचना होगा कि उन्होंने आवेदन पत्र के प्रत्येक संबंधित क्षेत्र में सही विवरण भरा है. ऑनलाइन आवेदन के लिए विंडो की समाप्ति के बाद, किसी भी परिस्थिति में कोई परिवर्तन/सुधार/संशोधन की अनुमति नहीं दी जाएगी. इस संबंध में डाक, ईमेल, हस्त सुपुर्दगी आदि किसी भी रूप में प्राप्त अनुरोधों पर विचार नहीं किया जाएगा और उन्हें तत्काल अस्वीकृत कर दिया जाएगा.
4. उम्मीदवारों की वैध ईमेल आईडी और मोबाइल फोन नंबर अवश्य हो जिसे परिणाम घोषित होने और अंतिम चयन पर कॉल लेटर जारी होने तक एक्टिव रखा जाए. इससे उन्हें ईमेल या मोबाइल पर एसएमएस द्वारा **कॉल लेटर/साक्षात्कार सूचना** आदि प्राप्त करने में सहायता होगी.
5. बैंक भर्ती किए गए/नियुक्त अधिकारियों की सेवाओं का तैनात करने/स्थानांतरण भारत में स्थित भारतीय स्टेट बैंक के किसी भी कार्यालय में करने या उन्हें अपने किन्हीं सहयोगियों/अनुषंगियों के पास या किसी अन्य संस्था के पास तैनात करने का अधिकार सुरक्षित रखता है, जो सेवा की आवश्यकताओं पर निर्भर होगा. किसी विशिष्ट स्थान/कार्यालय पर नियुक्ति/स्थानांतरण के अनुरोध पर विचार नहीं किया जाएगा.
6. उम्मीदवारों को सूचित किया जाता है कि वे अन्य विवरण एवं अद्यतन सूचना हेतु बैंक की वेबसाइट **https://sbi.bank.in/web/careers/current-openings** को नियमित रूप से देखें. **विज्ञापन में होने वाले किसी परिवर्तन/अद्यतन सूचना को अलग से विज्ञापित/सूचित नहीं किया जाएगा. सभी परिवर्तन/अपडेट/संशोधन/शुद्धिपत्र/परिणाम/शेड्यूल/शॉर्टलिस्ट किए गए/चयनित उम्मीदवारों की सूची आदि केवल बैंक की वेबसाइट पर ही उपलब्ध होंगे.** कॉल लेटर/सूचना, जहां भी आवश्यक हो, केवल ई-मेल द्वारा भेजी जाएगी **(कोई हार्ड कॉपी नहीं भेजी जाएगी).**
7. उम्मीदवारों को सभी आवश्यक दस्तावेज (जीवन वृत्त, पहचान का प्रमाण, आयु प्रमाण, जाति प्रमाण पत्र (यदि लागू हो), पीडब्ल्यूबीडी प्रमाण पत्र (यदि लागू हो), शैक्षणिक योग्यता, अन्य योग्यताएं/प्रमाणपत्र, अनुभव का प्रमाण आदि.) अपलोड करने की आवश्यकता है, ऐसा न करने पर उनके आवेदन/उम्मीदवारी पर शॉर्टलिस्टिंग/साक्षात्कार के लिए विचार नहीं किया जाएगा.
8. पद के लिए आवेदन करने वाले उम्मीदवारों को यह सुनिश्चित करना चाहिए कि भर्ती के सभी चरणों (जैसे शॉर्टलिस्टिंग, साक्षात्कार आदि) में उनका प्रवेश निर्धारित पात्रता शर्तों को पूरा करने के अधीन पूरी तरह से अनंतिम होगा. चयनित सूची दस्तावेज़ों के सत्यापन के बिना अनंतिम होगी. साक्षात्कार के समय (यदि बुलाया जाता है तो) उम्मीदवार द्वारा मूल प्रतियों सहित सभी विवरणों/दस्तावेज़ों का सत्यापन करवाए जाने पर ही उसकी उम्मीदवारी मानी जाएगी.
9. चयनित उम्मीदवारों को बैंक में नियोजन/नियुक्ति ऑफर की जा सकती है, बशर्ते कि वे अन्य औपचारिकताएं जैसे कि पात्रता, क्रेडेंशियल्स, प्रमाणपत्रों का सत्यापन, संदर्भों से संतोषजनक रिपोर्ट, चिकित्सा जाँच और पूर्ववृत्त का सत्यापन आदि पूरी करते हों.
10. आयु में छूट, शुल्क में छूट चाहने वाले उम्मीदवारों को उस समय निर्धारित प्रारूप में सक्षम प्राधिकारी का वैध अपेक्षित प्रमाण पत्र प्रस्तुत करना होगा, जब दस्तावेज़ सत्यापन के समय ऐसा प्रमाण पत्र मांगा जाता है. अन्यथा, उनके दावे पर विचार नहीं किया जाएगा और उनकी उम्मीदवारी रद्द/अस्वीकृत कर दी जाएगी.
11. उम्मीदवार जिनके खिलाफ चरित्र और पूर्ववृत्त (कैरेक्टर एंड एंटीसिडण्टस), नैतिकता आदि के बारे में प्रतिकूल रिपोर्ट हैं, वह भी इस पद के लिए आवेदन करने के लिए पात्र नहीं हैं. यदि शॉर्टलिस्ट किए गए/चयनित उम्मीदवारों के विरुद्ध ऐसे कोई भी प्रतिकूल आदेश/रिपोर्ट उनके चयन के बाद बैंक को मिलती/प्राप्त होती है, तो उनकी उम्मीदवारी/सेवा तुरंत समाप्त कर दी जाएगी.
12. **उम्मीदवार को दो से अधिक पद के लिए आवेदन करने की अनुमति नहीं है.**
13. यदि किसी उम्मीदवार द्वारा एक ही पद/एकाधिक पदों के लिए एक से अधिक आवेदन (बहु आवेदन) प्रस्तुत किए जाते हैं, तो केवल अंतिम वैध (पूर्ण) आवेदन ही रखा जाएगा, और अन्य पंजीकरणों के लिए प्रदत्त आवेदन शुल्क आदि जब्त कर लिया जाएगा. इसके अलावा, साक्षात्कार/कार्यग्रहण के समय एक उम्मीदवार द्वारा एकाधिक हाजिरी/उपस्थिति की परिणति उम्मीदवारी को सरासरी तौर पर अस्वीकृति/रद्दीकरण में होगी.
14. यदि कोई उम्मीदवार दो से अधिक पदों के लिए आवेदन करता है, तो केवल दो अलग-अलग पदों के लिए अंतिम वैध (पूर्ण) आवेदन ही रखा जाएगा, और अन्य पंजीकरणों के लिए भुगतान किया गया आवेदन शुल्क (यदि कोई हो) जब्त कर लिया जाएगा
15. बैंक बिना कोई कारण बताए, आरक्षित रिक्तियों सहित अधिसूचित रिक्तियों को बदलने का अधिकार सुरक्षित रखता है.
16. बैंक बिना कोई कारण बताए किसी भी विशेष पद/सभी पदों के लिए किसी भी स्तर/समय पर भर्ती प्रक्रिया को पूरी तरह या आंशिक रूप से रद्द/संशोधित करने, यदि ऐसा आवश्यक हो, का अधिकार सुरक्षित रखता है, और बैंक आवेदक को शुल्क वापस करने या कोई मुआवजा देने के लिए उत्तरदायी नहीं होगा.
17. गलत जानकारी प्रस्तुत करने/तथ्यों को छिपाने वाले उम्मीदवारों को अयोग्य घोषित कर दिया जाएगा और उन पर प्रतिबंध लगाया जा सकता है और कानूनी/आपराधिक कार्रवाई की जा सकती है. जो उम्मीदवार धोखाधड़ी/छद्मव्यक्तिता का प्रयास करेंगे, उन्हें बैंक द्वारा आयोजित भविष्य की भर्ती प्रक्रिया से वंचित कर दिया जाएगा.
18. चयनित उम्मीदवार, नियुक्ति के बाद, संबंधित पदों के लिए समय-समय पर लागू/संशोधित/आशोधित बैंक की मौजूदा भर्ती नीति के अनुसार परिवीक्षा पर होंगे.
19. इस परियोजना के तहत सभी नियुक्तियाँ पूरी तरह से बैंक के विवेकाधिकार पर होंगी और पद के लिए स्वीकार्य वेतनमान के प्रारंभिक चरण में की जाएंगी.
20. यदि उम्मीदवारों को शॉर्टलिस्ट किया जाता है, तो बैंक साक्षात्कार के लिए स्थान/केंद्र तय करेगा. यदि उम्मीदवारों को बुलाया जाता है, तो उन्हें बैंक द्वारा निर्धारित केंद्र/स्थान पर साक्षात्कार के लिए उपस्थित होना होगा और इस संबंध में किसी भी अनुरोध पर बैंक द्वारा विचार नहीं किया जाएगा.
21. यदि उम्मीदवार को साक्षात्कार के लिए बुलाया जाता है और यदि वह पात्रता मानदंडों (आयु, शैक्षणिक योग्यता, अन्य योग्यता और अनुभव आदि) को पूरा नहीं करता/करती है तो उसे न तो साक्षात्कार में उपस्थित होने दिया जाएगा और न ही वह यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे.
22. यदि अंतिम मेरिट लिस्ट (कट-ऑफ अंक पर समान अंक) में एक से अधिक उम्मीदवारों के कट-ऑफ अंकों के रूप में एकसमान अंक आते हैं, तो ऐसे उम्मीदवारों को मेरिट में उनकी आयु के अनुसार अवरोही क्रम में स्थान दिया जाएगा.
23. किसी पत्र के मिलने में विलंब होने या न मिलने के लिए बैंक की कोई जिम्मेदारी नहीं होगी.

24. जो उम्मीदवार सरकार/अर्ध-सरकारी कार्यालयों, बैंकों और वित्तीय संस्थानों सहित सार्वजनिक क्षेत्र के प्रतिष्ठानों में कार्यरत हैं, उन्हें सूचना दी जाती है कि वे **साक्षात्कार के समय अपने नियोक्ता से अनापत्ति प्रमाणपत्र लेकर प्रस्तुत करें, ऐसा न करने पर उनकी उम्मीदवारी पर विचार नहीं किया जाएगा** और वे यदि किसी यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे, तो उन्हें उसका भुगतान नहीं किया जाएगा.

25. चयन की दशा में, उम्मीदवार से अपेक्षा होगी कि वह नियुक्ति प्राप्त करते समय अपने वर्तमान नियोक्ता का उचित डिस्चार्ज बुक प्रस्तुत करें.

26. **सिबिल (CIBIL):** जिन उम्मीदवारों ने क्रेडिट कार्ड की बकाया राशि सहित बैंकों/एनबीएफसी/वित्तीय संस्थाओं के साथ किसी भी उधार व्यवस्था के तहत चुकौती में चूक की है और बैंक द्वारा नियोजन/नियुक्ति प्रस्ताव पत्र जारी करने की तारीख तक उनके बकाया को नियमित/चुकाया नहीं है, वे पद पर नियोजन/नियुक्ति के लिए पात्र नहीं होंगे. हालांकि, ऐसे उम्मीदवार जिन्होंने नियोजन/नियुक्ति प्रस्ताव-पत्र जारी होने की तारीख को या उससे पहले इस तरह के बकाया को नियमित कर लिया है/चुका दिया है, लेकिन जिनकी **सिबिल (CIBIL)** स्थिति को **शामिल होने की तारीख को या उससे पहले** अपडेट नहीं किया गया है, उन्हें या तो सिबिल की स्थिति को अपडेट कराना होगा या ऋणदाता से इस आशय का अनापत्ति प्रमाण-पत्र प्रस्तुत करना होगा कि सिबिल में प्रतिकूल रूप से दर्शाए गए खातों के संबंध में कोई बकाया नहीं है, ऐसा न करने पर प्रस्ताव पत्र वापस ले लिया जाएगा/रद्द कर दिया जाएगा. इस प्रकार, ऋण/क्रेडिट कार्ड बकाए के भुगतान में चूक के रिकॉर्ड और/या जिनके नाम पर सिबिल या अन्य बाहरी एजेंसियों की प्रतिकूल रिपोर्ट उपलब्ध है, ऐसे उम्मीदवार नियोजन/नियुक्ति के लिए पात्र नहीं हैं.

क. पद/नियुक्ति की प्रकृति/श्रेणी/रिक्तियाँ/आयु का विवरण:

क्र. सं.	पद का नाम और प्रकार	नियुक्ति की प्रकृति/श्रेणी	रिक्तियाँ			पीडब्ल्यूबीडी #	आयु वर्षों में^ (31.12.2025 तक)	
			अनारक्षित	अ.पि.व.	कुल	वीआई	न्यूनतम	अधिकतम
1.	उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ	नियमित (एमएमजीएस-II)	1	--	**1**	--	25	35
2.	उप प्रबंधक – उभरती प्रौद्योगिकी		3	1	**4**	1		
3.	उप प्रबंधक – साइबर सुरक्षा विश्लेषक		2	--	**2**	1		
4.	उप प्रबंधक – घटना प्रबंधन और फोरेंसिक		2	--	**2**	1		
5.	उप प्रबंधक – परीक्षण इंजीनियर		3	--	**3**	1		
	कुल		**11**	1	**12**	4		

- समस्तरीय रिक्तियाँ.

^ भारत सरकार के दिशानिर्देशों के अनुसार आयु में छूट उपलब्ध है.

संक्षेपाक्षर: यूआर – अनारक्षित; **पीडब्ल्यूबीडी –** निर्धारित दिव्यांगता वाले उम्मीदवार; **अ.पि.व. (ओबीसी)**– अन्य पिछड़ा वर्ग; **वीआई –** दृष्टि बाधित;

महत्वपूर्ण बिंदु:

1. पीडब्ल्यूबीडी उम्मीदवारों के लिए आरक्षण समस्तरीय है और संबंधित मूल श्रेणी की समग्र रिक्ति में शामिल है.
2. ऊपर उल्लिखित आरक्षित रिक्त-पदों सहित रिक्तियों की संख्या **अनंतिम है** और यह बैंक की वास्तविक आवश्यकता के अनुसार **बदल सकती है.**
3. चयनित उम्मीदवारों की तैनाती/प्लेसमेंट/उपयोग बैंक के पूर्ण विवेकाधिकार पर किया जाएगा.
4. इंगित अधिकतम आयु अनारक्षित श्रेणी के उम्मीदवारों के लिए है. आरक्षित श्रेणी के उम्मीदवारों को भारत सरकार के दिशा-निर्देशों के अनुसार **ऊपरी आयु सीमा में छूट** उपलब्ध है (जहां लागू हो).
5. विभिन्न श्रेणियों के तहत आरक्षण भारत सरकार दिशानिर्देशों के अनुसार होगा.
6. ऐसे उम्मीदवार जो ओबीसी श्रेणी से संबंधित हैं लेकिन 'क्रीमी लेयर' से आते हैं, वे ओबीसी आरक्षण एवं आयु छूट के लिए पात्र नहीं होंगे. उन्हें अपनी श्रेणी 'यूआर' या यूआर (पीडब्ल्यूबीडी), के रूप में दर्शाना चाहिए.
7. ओबीसी श्रेणी के अंतर्गत आरक्षण माँगने वाले उम्मीदवारों द्वारा निर्धारित प्रारूप में एक घोषणा जमा करवानी होगी कि वह आवेदन के ऑनलाइन पंजीकरण की आखरी तिथि को क्रीमी लेयर से नहीं है. **यदि उन्हें साक्षात्कार के लिए बुलाया जाता है, तो ऐसे उम्मीदवारों को 01.04.2025 से साक्षात्कार की तिथि के दौरान जारी किया गया 'नॉन क्रीमी लेयर' अनुच्छेद वाला ओबीसी प्रमाण-पत्र, जमा करना चाहिए.** उक्त तारीख के बाद 'प्रमाणपत्र' प्रस्तुत करने के लिए समय बढ़ाने के किसी भी अनुरोध पर विचार नहीं किया जाएगा और उम्मीदवारी रद्द कर दी जाएगी.
8. निर्धारित दिव्यांग व्यक्ति (पीडब्ल्यूबीडी), जिनके लिए कोई आरक्षण का उल्लेख नहीं किया गया है, सहित आरक्षित श्रेणी से संबंधित उम्मीदवार अनारक्षित श्रेणी के लिए घोषित रिक्तियों के लिए आवेदन करने के लिए स्वतंत्र हैं, बशर्ते वे अनारक्षित श्रेणी के लिए लागू सभी पात्रता मानदंडों को पूरा करते हों.
9. पीडब्ल्यूबीडी श्रेणी सहित आरक्षित श्रेणी (अर्थात एससी, एसटी, ओबीसी) के तहत आरक्षण/छूट का लाभ केवल **भारत सरकार द्वारा निर्धारित प्रारूप पर** सक्षम प्राधिकारी द्वारा जारी वैध जाति प्रमाण पत्र प्रस्तुत करने पर ही उठाया जा सकता है.
10. ऊपरी आयु सीमा में छूट निम्नानुसार होगी **(जहां लागू हो):**

क्र.	श्रेणी		आयु में छूट (वर्षों में)
क)	अन्य पिछड़े वर्ग (अपिव) (नॉन क्रीमी लेयर)		3
ख)	अनुसूचित जाति/अनुसूचित जनजाति (अजा/अजजा)		5
ग)	बेंचमार्क दिव्यांगता वाले व्यक्ति (पीडब्ल्यूबीडी)	– पीडब्ल्यूबीडी (अना/ईडब्ल्यूएस)	10
		– पीडब्ल्यूबीडी (अपिव)	13
		– पीडब्ल्यूबीडी (अजा/अजजा)	15

टिप्पणी: आयु सीमा संबंधी छूट उपर्युक्त मदों या विभिन्न मदों के अंतर्गत दर्शायी गई अन्य आयु सीमा की छूटों को मिलाकर नहीं दी जाएगी. आयु में छूट चाहने वाले उम्मीदवारों को शॉर्टलिस्ट किए जाने पर समूह अभ्यास/साक्षात्कार के समय आवश्यक प्रमाणपत्रों की प्रतियां प्रस्तुत करनी होंगी. ऑनलाइन आवेदन पंजीकरण के पश्चात, किसी उम्मीदवार की श्रेणी में कोई परिवर्तन संभव नहीं है. इस संबंध में किसी पत्र-व्यवहार/ ई-मेल/फोन पर विचार नहीं किया जाएगा.

11. पीडब्ल्यूबीडी उम्मीदवार को भारत सरकार के दिशानिर्देशों के अनुसार सक्षम प्राधिकारी द्वारा जारी प्रमाणपत्र प्रस्तुत करना होगा.
12. केवल **निर्धारित दिव्यांगता** वाले व्यक्ति ही निर्धारित दिव्यांगता (PwBD) श्रेणी के तहत आरक्षण के लिए पात्र होंगे. **'निर्धारित दिव्यांगता वाले व्यक्ति'** से आशय उस व्यक्ति से है जो विनिर्दिष्ट दिव्यांगता का कम से कम 40 प्रतिशत दिव्यांग हो, उन मामलों में जहाँ विनिर्दिष्ट दिव्यांगता को मापन श्रेणी में नहीं रखा गया है. तथा इसके अंतर्गत वह दिव्यांग व्यक्ति भी आता है जिसकी दिव्यांगता को प्रमाणित करने वाले प्राधिकारी के प्रमाणन के अनुसार मापन श्रेणी में रखा गया है. आरक्षण का लाभ उठाने के इच्छुक व्यक्ति को चिकित्सा प्राधिकारी या किसी अन्य अधिसूचित सक्षम प्राधिकारी (प्रमाणकर्त्ता प्राधिकारी) द्वारा निर्धारित प्रारूप पर जारी नवीनतम दिव्यांगता प्रमाण पत्र जमा करना होगा. **प्रमाणपत्र आवेदन के पंजीकरण की अंतिम तिथि या उससे पहले का होना चाहिए. वैध प्रमाण पत्र के अभाव में, उम्मीदवारी बैंक द्वारा रद्द/स्वीकार नहीं की जाएगी और इस संबंध में किसी भी पत्र-व्यवहार पर बैंक द्वारा विचार नहीं किया जाएगा.** दिव्यांग जन अधिकार अधिनियम 2016 की धारा 34 के अनुसार निर्धारित दिव्यांगता वाले व्यक्तियों को समस्तरीय आरक्षण दिया गया है. पद के लिए दिव्यांगता की उपयुक्त श्रेणियां और कार्यात्मक अपेक्षाएं भारत के राजपत्र, अधिसूचना संख्या 38-16/2020-डीडी-III दिनांक 4 जनवरी 2021, सामाजिक न्याय और अधिकारिता मंत्रालय दिव्यांगजन सशक्तिकरण विभाग के संदर्भ में होंगी.

ख. शैक्षणिक योग्यता/प्रमाणपत्र/कार्य अनुभव/आवश्यक विशिष्ट कौशल का विवरण:

पद संख्या/पद नाम	1 - उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ
मूल योग्यता (31.01.2026 तक)	**अनिवार्य:** कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री, **न्यूनतम 50% अंकों के साथ.** अथवा एम.सी.ए. अथवा कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सूचना प्रौद्योगिकी/सॉफ्टवेयर इंजीनियरिंग/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/एम.एससी या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री. (भारत सरकार द्वारा मान्यताप्राप्त/सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/संस्थान/बोर्ड से) **वरीयता:** **साइबर सुरक्षा या सूचना प्रौद्योगिकी में उच्च डिग्री को प्राथमिकता दी जाएगी.**
अन्य योग्यता (31.01.2026 तक)	**वरीयता प्रमाणपत्र:** (दिनांक 31.01.2026 को वैध) ओएससीपी, सीईएच, सीएचएफआई, जीआईएफआर, जीआईएसीसी, जीएफएसयू (OSCP, CEH, CHFI, GIFR, GIACC, GFSU) प्रमाणपत्र.
कार्य अनुभव (मूल योग्यता के बाद) (31.01.2026 तक)	**अनिवार्य:** न्यूनतम अनुभवः साइबर सुरक्षा/सूचना प्रौद्योगिकी क्षेत्र में योग्यता–पश्चात् 4 वर्ष का अनुभव. **वरीयता:** साइबर सुरक्षा संचालन (थ्रेट इंटेलिजेंस), घटना प्रतिक्रिया, मैलवेयर विश्लेषण, फोरेंसिक और थ्रेट हंटिंग में अनुभव. **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.** **नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया होः (i) नौकरी की प्रकृति, (ii) अनुभव की तिथियां और अवधि, (iii) स्तर/पद, (iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि. हालाँकि, यदि उम्मीदवार ऊपर बताए गए अनुसार अनुभव प्रमाण पत्र प्रस्तुत करने में असमर्थ है, तो अनुभव, कार्य की प्रकृति और दावा की गई अवधि को स्पष्ट रूप से दर्शाने वाला कोई भी दस्तावेज़ प्रस्तुत किया जा सकता है और बैंक के विवेक पर गुणों के आधार पर उस पर विचार किया जाएगा और बैंक का निर्णय अंतिम होगा.
विशिष्ट कौशल:	• घटना प्रतिक्रिया, मैलवेयर विश्लेषण, डिजिटल फोरेंसिक और साइबर थ्रेट हंटिंग में विशेषज्ञता. • क्लाउड, ओटी/आईसीएस और आईओटी सुरक्षा, रेड टीमिंग, आईआर और एथिकल हैकिंग की समझ. • मजबूत तकनीकी नेतृत्व, मानव संसाधन प्रबंधन और हितधारकों के साथ प्रभावी जुड़ाव कौशल. • उच्च दबाव वाली साइबर संकट स्थितियों को संभालने की क्षमता. • उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल, जिसमें वरिष्ठ अधिकारियों और नीति निर्माताओं को संक्षिप्त जानकारी देने की क्षमता शामिल है.

पद संख्या/पद नाम	2 - उप प्रबंधक – उभरती प्रौद्योगिकी
मूल योग्यता (31.01.2026 तक)	**अनिवार्य:** कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री, **न्यूनतम 50% अंकों के साथ.** अथवा एम.सी.ए. अथवा कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सूचना प्रौद्योगिकी/सॉफ्टवेयर इंजीनियरिंग/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/एम.एससी या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री. (भारत सरकार द्वारा मान्यताप्राप्त/सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/संस्थान/बोर्ड से) **वरीयता:** **साइबर सुरक्षा या सूचना प्रौद्योगिकी में उच्च डिग्री को प्राथमिकता दी जाएगी.**
अन्य योग्यता (31.01.2026 तक)	**वरीयता प्रमाणपत्र:** (दिनांक 31.01.2026 को वैध) • साइबर सुरक्षा में नवाचार, उत्पाद विकास, वेब विकास आदि में समकक्ष प्रमाणपत्र. • जावा डेवलपर, मोबाइल डेवलपर, पायथन डेवलपर, वेब डेवलपर.
कार्य अनुभव (मूल योग्यता के बाद) (31.01.2026 तक)	**अनिवार्य:** न्यूनतम अनुभवः साइबर सुरक्षा/टेक्नोलॉजी इनोवेशन क्षेत्र में योग्यता–पश्चात् 4 वर्ष का अनुभव. **वरीयता:** व्यावहारिक कार्य अनुभव, अधिमानतः साइबर नवाचार प्रयोगशालाओं में. उत्पाद मूल्यांकन, प्रोटोटाइपिंग या अनुप्रयुक्त साइबर सुरक्षा समाधान विकसित करने का अनुभव वांछनीय है. अनुसंधान एवं विकास या अनुप्रयुक्त प्रौद्योगिकी संबंधी समस्याओं को हल करने का अनुभव और नवाचार परिवेश में कार्य अनुभव अतिरिक्त लाभ है. साइबर अनुसंधान, खतरे की खुफिया जानकारी अनुसंधान आदि. साइबर सुरक्षा सिद्धांतों, खतरे के परिदृश्यों और सूचना सुरक्षा प्रौद्योगिकियों की समझ. **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**

	नोट: उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो: (i) कार्य की प्रकृति, (ii) अनुभव की तिथियां और अवधि, (iii) स्तर/पद, (iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि. हालाँकि, यदि उम्मीदवार ऊपर बताए गए अनुसार अनुभव प्रमाण पत्र प्रस्तुत करने में असमर्थ है, तो अनुभव, कार्य की प्रकृति और दावा की गई अवधि को स्पष्ट रूप से दर्शाने वाला कोई भी दस्तावेज़ प्रस्तुत किया जा सकता है और बैंक के विवेक पर गुणों के आधार पर उस पर विचार किया जाएगा और बैंक का निर्णय अंतिम होगा.
विशिष्ट कौशल:	• जटिल सुरक्षा चुनौतियों के लिए रचनात्मक रूप से सोचने और मौलिक, प्रभावी समाधान विकसित करने की क्षमता. • सुरक्षा घटनाओं का विश्लेषण करने और नई प्रौद्योगिकियों और रणनीतियों की प्रभावशीलता का आकलन करने की प्रबल क्षमता. • अत्याधुनिक प्रौद्योगिकियों और उभरते खतरों से अवगत रहने के लिए निरंतर सीखने की मानसिकता. • उभरती प्रौद्योगिकियों की प्रबल समझ: कृत्रिम बुद्धिमत्ता (एआई/एमएल), ब्लॉकचेन, क्वांटम कंप्यूटिंग, क्लाउड सुरक्षा. • साइबर खतरे की मॉडलिंग, सिमुलेशन और परिदृश्य-आधारित मूल्यांकन में दक्षता. • प्रोटोटाइपिंग, उत्पाद सत्यापन और व्यावहारिक अनुसंधान में क्षमता. • स्टार्टअप्स, शैक्षणिक संस्थानों और फिनटेक नवप्रवर्तकों के साथ मिलकर समाधान विकसित करने की क्षमता. • उत्कृष्ट विश्लेषणात्मक, तकनीकी लेखन और प्रस्तुति कौशल. • बैंक की साइबर सुरक्षा नीति के अनुरूप नवाचार को लागू करने योग्य समाधानों में रूपांतरित करने की क्षमता. • बैंकिंग, वित्तीय संस्थानों (एफआई) या सार्वजनिक क्षेत्र के उपक्रमों (पीएसयू) के नेतृत्व वाले साइबर सुरक्षा नवाचार परियोजनाओं का अनुभव. • उभरती प्रौद्योगिकी/साइबर सुरक्षा नवाचार में अकादमिक संस्थानों, स्टार्टअप्स और इनक्यूबेटर्स के साथ सहयोग. • प्रौद्योगिकी/साइबर सुरक्षा में राष्ट्रीय/अंतर्राष्ट्रीय अनुसंधान पहलों या पेटेंट में योगदान करने की क्षमता. • उभरते साइबर खतरों, टूल्स और प्रवृत्तियों पर गहन शोध करने की क्षमता. • ओपन-सोर्स इंटेलिजेंस (OSINT) उपकरणों और तकनीकों का अनुभव. • तकनीकी और गैर-तकनीकी स्रोतों से डेटा संग्रह, संश्लेषण और व्याख्या. • नेटवर्क सुरक्षा, क्लाउड सुरक्षा, एंडपॉइंट सुरक्षा और घटना प्रतिक्रिया सहित साइबर सुरक्षा सिद्धांतों, प्रौद्योगिकियों और सर्वोत्तम प्रथाओं की समझ. • दुर्भावनापूर्ण तत्वों द्वारा दुरुपयोग किए जाने से पहले सिस्टम, एप्लिकेशन और नेटवर्क में सुरक्षा खामियों का पता लगाना. • सुरक्षा समाधानों की आवश्यकता को सिद्ध करने में सहायक, कमजोरियों के वास्तविक प्रभाव को प्रदर्शित करने के लिए प्रूफ-ऑफ-कॉन्सेप्ट एक्सप्लॉइट्स विकसित करना. • जटिल साइबर सुरक्षा चुनौतियों से निपटने के लिए अनुसंधान करने, डेटा का विश्लेषण करने और नवीन समाधानों या विचारों की पहचान करने की क्षमता. • तकनीकी और गैर-तकनीकी दोनों तरह के श्रोताओं को जटिल तकनीकी जानकारी प्रभावी ढंग से संप्रेषित करने की क्षमता. • जटिल साइबर सुरक्षा समस्याओं की पहचान करने और उन्हें हल करने की क्षमता. • सिस्टम कैसे काम करते हैं, इसे समझने की गहरी जिज्ञासा और जटिल समस्याओं की जांच करने की लगन.

पद संख्या/पद नाम	**3 - उप प्रबंधक – साइबर सुरक्षा विश्लेषक**
मूल योग्यता (31.01.2026 तक)	**अनिवार्य:** कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री, **न्यूनतम 50% अंकों के साथ.** अथवा एम.सी.ए. अथवा कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सूचना प्रौद्योगिकी/सॉफ्टवेयर इंजीनियरिंग/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/एम.एससी या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री. (भारत सरकार द्वारा मान्यताप्राप्त/सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/संस्थान/बोर्ड से) **वरीयता:** **साइबर सुरक्षा या सूचना प्रौद्योगिकी में उच्च डिग्री को प्राथमिकता दी जाएगी.**
अन्य योग्यता (31.01.2026 तक)	**वरीयता प्रमाणपत्र:** (दिनांक 31.01.2026 को वैध) ओएससीपी, ओएससीई, सीआरटीई, सीआरटीपी, सीईएच, सीआईएसएसपी, ओएसईपी, सीसीएसपी, एसएनएनएस (OSCP, OSCE, CRTE, CRTP, CEH, CISSP, OSEP, CCSP, SANS) प्रमाणपत्र.
कार्य अनुभव (मूल योग्यता के बाद) (31.01.2026 तक)	**अनिवार्य:** न्यूनतम अनुभव: साइबर सुरक्षा/सूचना प्रौद्योगिकी क्षेत्र में योग्यता-पश्चात् 4 वर्ष का अनुभव. **वरीयता:** एथिकल हैकिंग, रेड टीमिंग और पेनिट्रेशन टेस्टिंग पर फोकस करते हुए आक्रामक सुरक्षा में अनुभव. **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.** **नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो: (i) कार्य की प्रकृति, (ii) अनुभव की तिथियां और अवधि, (iii) स्तर/पद, (iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि. हालाँकि, यदि उम्मीदवार ऊपर बताए गए अनुसार अनुभव प्रमाण पत्र प्रस्तुत करने में असमर्थ है, तो अनुभव, कार्य की प्रकृति और दावा की गई अवधि को स्पष्ट रूप से दर्शाने वाला कोई भी दस्तावेज़ प्रस्तुत किया जा सकता है और बैंक के विवेक पर गुणों के आधार पर उस पर विचार किया जाएगा और बैंक का निर्णय अंतिम होगा.

विशिष्ट कौशल:	• वेब/मोबाइल एप्लिकेशन और नेटवर्क सुरक्षा से संबंधित आईटी सुरक्षा प्रौद्योगिकीयों और प्रक्रियाओं की समझ. • OWASP वेब और मोबाइल टॉप 10 एप्लिकेशन सुरक्षा कमजोरियों, थ्रेट मॉडलिंग, रेड टीमिंग और सुरक्षित कोड समीक्षा की समझ. • OWASP टॉप 10 से संबंधित कमजोरियों की पहचान करने के लिए वेब और मोबाइल (एंड्रॉइड और आईओएस) एप्लिकेशन का सुरक्षा मूल्यांकन करने की क्षमता. • काली लिनक्स, बर्प सूट, एनमैप, क्वालिस/नेसस, मेटास्प्लॉइट, एचसीएल ऐपस्कैन, टेनेबल एससी, एनएमएपी आदि जैसे टूल का ज्ञान. • C, C++, पायथन, जावा, ASP.NET जैसी कम से कम एक प्रोग्रामिंग भाषा के बुनियादी ज्ञान को वरीयता दी जाएगी. • मोबाइल एप्लिकेशन की सुरक्षा जांच (स्थैतिक/गतिशील/मेमोरी विश्लेषण) का व्यावहारिक अनुभव और फ्रिडा/ऑब्जेक्शन, मैजिस्क आदि जैसे गतिशील इंस्ट्रूमेंटेशन टूल्स का ज्ञान. एंड्रॉइड डेवलपमेंट टूल्स का ज्ञान. • पायथन, बैश/शेल, C/C++, जावा और जावास्क्रिप्ट जैसी भाषाओं में दक्षता. बर्प सूट, काली–लिनक्स स्क्रिप्टिंग, ऑटोमेशन, एक्सप्लॉइट डेवलपमेंट और सिस्टम कमजोरियों को समझने के लिए अनिवार्य है. • विभिन्न पेनिट्रेशन टेस्टिंग और रेड टीम टेस्टिंग पद्धतियों (एमआईटीआरई, ओडब्ल्यूएएसपी टेस्टिंग गाइड, एनआईएसटी एसपी 800-115, आदि), टूल्स (एनमैप, मेटास्प्लॉइट, बर्प सूट, वायरशार्क, जॉन द रिपर, आदि) और तकनीकों (रिकॉनसेंस, स्कैनिंग, एक्सप्लॉइटेशन, पोस्ट–एक्सप्लॉइटेशन, प्रिविलेज एस्केलेशन) में विशेषज्ञता. • वायरलेस प्रोटोकॉल (वाई–फाई), सुरक्षा मानक (WPA2, WPA3) और हैकिंग विधियों (पैकेट स्निफिंग, एन्क्रिप्शन क्रैकिंग) का ज्ञान. • जटिल परिस्थितियों का विश्लेषण करने, चुनौतियों की पहचान करने और आलोचनात्मक एवं रचनात्मक सोच के माध्यम से प्रभावी और नवीन समाधान निकालने की क्षमता, साथ ही संभावित सुरक्षा जोखिमों को पहचानने की कुशलता.

पद संख्या/पद नाम	**4 - उप प्रबंधक – घटना प्रबंधन और फोरेंसिक**
मूल योग्यता (31.01.2026 तक)	**अनिवार्य:** कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री, **न्यूनतम 50% अंकों के साथ.** अथवा एम.सी.ए. अथवा कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सूचना प्रौद्योगिकी/सॉफ्टवेयर इंजीनियरिंग/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/एम.एससी या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री. (भारत सरकार द्वारा मान्यताप्राप्त/सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/संस्थान/बोर्ड से) **वरीयता:** **साइबर सुरक्षा या सूचना प्रौद्योगिकी में उच्च डिग्री को प्राथमिकता दी जाएगी.**
अन्य योग्यता (31.01.2026 तक)	**वरीयता प्रमाणपत्र:** (दिनांक 31.01.2026 को वैध) सीएचएफआई, एनकेस सर्टिफाइड एग्जामिनर (EnCE), एक्सेस डेटा सर्टिफाइड एग्जामिनर (ACE), GIAC सर्टिफाइड इंसिडेंट हैंडलर (GCIH), सर्टिफाइड इंफॉर्मेशन सिस्टम्स सिक्योरिटी प्रोफेशनल (CISSP), GIAC सर्टिफाइड फोरेंसिक एनालिस्ट (GCFA), सीईएच, ओएससीपी, ओसीईपी.
कार्य अनुभव (मूल योग्यता के बाद) (31.01.2026 तक)	**अनिवार्य:** न्यूनतम अनुभव: साइबर सुरक्षा/सूचना प्रौद्योगिकी क्षेत्र में योग्यता–पश्चात् 4 वर्ष का अनुभव. **वरीयता:** घटना प्रतिक्रिया, फोरेंसिक और मैलवेयर विश्लेषण में अनुभव. मैलवेयर विश्लेषण, डिजिटल फोरेंसिक, मोबाइल फोरेंसिक, नेटवर्क फोरेंसिक, डेटाबेस फोरेंसिक, ईमेल फोरेंसिक, क्लाउड फोरेंसिक में व्यावहारिक अनुभव ओर घटना प्रतिक्रिया और सुरक्षा संचालन पर केंद्रित साइबर सुरक्षा में अनुभव. मालवेयर, रैंसमवेयर, फ़िशिंग, डीडीओएस हमले और डेटा उल्लंघन जैसी विभिन्न सुरक्षा घटनाओं का अनुभव. **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.** **नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो: (i) कार्य की प्रकृति, (ii) अनुभव की तिथियां और अवधि, (iii) स्तर/पद, (iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि. हालाँकि, यदि उम्मीदवार ऊपर बताए गए अनुसार अनुभव प्रमाण पत्र प्रस्तुत करने में असमर्थ है, तो अनुभव, कार्य की प्रकृति और दावा की गई अवधि को स्पष्ट रूप से दर्शाने वाला कोई भी दस्तावेज़ प्रस्तुत किया जा सकता है और बैंक के विवेक पर गुणों के आधार पर उस पर विचार किया जाएगा और बैंक का निर्णय अंतिम होगा.
विशिष्ट कौशल:	**मूल फोरेंसिक कौशल** • **डिजिटल फोरेंसिक्स:** उपकरणों, सर्वरों और नेटवर्कों से डिजिटल साक्ष्य प्राप्त करने, संरक्षित करने, विश्लेषण करने और रिपोर्ट करने में विशेषज्ञता. • पता लगाना और जांच: धनशोधन, भेदिया कारोबार और साइबर धोखाधड़ी जैसी धोखाधड़ी योजनाओं का पता लगाने, जांच करने और दस्तावेजीकरण करने का गहन ज्ञान. • घटना प्रतिक्रिया: डेटा उल्लंघनों, साइबर घटनाओं और सुरक्षा खतरों की कुशलतापूर्वक जांच और निष्पादन करने की क्षमता. **तकनीकी कौशल** • **फ़ोरेंसिक टूल्स में विशेषज्ञता:** एनकेस, FTK, Magnet Axiom, X-Ways, ऑटोप्सी, वायरशार्क, सेलेब्राइट, ऑक्सीजन फोरेंसिक्स (मोबाइल फ़ोरेंसिक्स के लिए) आदि। • फ़ोरेंसिक इमेजिंग टूल्स: टेबलू TX1/TDU/राइट ब्लॉकर, लॉजिक्यूड इमेज आदि। • एसआईईएम और थ्रेट इंटेलिजेंस टूल्स: स्प्लंक, आईबीएम क्यूराडार, आर्कसाइट • डेटा विश्लेषण और स्क्रिप्टिंग: कोर बैंकिंग सिस्टम से डेटा निकालने के लिए SQL • स्क्रिप्टिंग और ऑटोमेशन के लिए पायथन और पॉवरशेल • मैलवेयर विश्लेषण और रिवर्स इंजीनियरिंग (साइबर फ़ोरेंसिक्स भूमिकाओं के लिए वरीयता)

	बीएफएसआई, विनियामक और कानूनी क्षेत्र का ज्ञान • वित्तीय उत्पादों और प्रणालियों की समझ • साइबर सुरक्षा और फोरेंसिक से संबंधित आरबीआई के दिशानिर्देश • सेबी और आईआरडीएआई के विनियम • अभिरक्षा श्रृंखला: कानूनी रूप से मान्य साक्ष्यों का रिकॉर्ड बनाए रखने की क्षमता • रिपोर्ट लेखन: विस्तृत फोरेंसिक रिपोर्ट और कार्यपालक सारांश तैयार करने का कौशल. • उत्कृष्ट संप्रेषण और प्रस्तुति कौशल. तकनीकी और गैर–तकनीकी दोनों तरह के श्रोताओं को तकनीकी जानकारी प्रभावी ढंग से संप्रेषित करने की क्षमता. • नेटवर्क प्रोटोकॉल और ऑपरेटिंग सिस्टम का ज्ञान. • मैलवेयर विश्लेषण, डिजिटल फोरेंसिक्स, मोबाइल फोरेंसिक्स, नेटवर्क फोरेंसिक्स, डेटाबेस फोरेंसिक्स, ईमेल फोरेंसिक्स और क्लाउड फोरेंसिक में व्यावहारिक अनुभव. • साइबर सुरक्षा घटनाओं के संपूर्ण जीवनचक्र का निष्पादन और समन्वय – पहचान, रोकथाम, उन्मूलन, पुनर्प्राप्ति और घटना के बाद का विश्लेषण. • मैलवेयर हमले, डीडीओएस हमले, रैंसमवेयर, फ़िशिंग, डेटा उल्लंघन और आंतरिक खतरों सहित उच्च गंभीरता वाली सुरक्षा घटनाओं के लिए प्राथमिक प्रतिक्रियाकर्ता के रूप में कार्य करना. • एंडपॉइंट्स, नेटवर्क और एप्लिकेशन में विसंगतियों और संभावित खतरों का पता लगाने के लिए SIEM टूल्स (जैसे, स्प्लंक, क्यूराडार, आर्कसाइट) से लॉग और अलर्ट की निगरानी और विश्लेषण करें. • आरबीआई के साइबर सुरक्षा निर्देशों के अनुरूप घटना प्लेबुक, एस्केलेशन प्रोटोकॉल और रिस्पॉन्स कार्य–प्रवाह विकसित करना और बनाए रखें. • प्रभावित सिस्टमों पर फोरेंसिक विश्लेषण करके मूल कारण, प्रभाव और कॉम्प्रोमाइज़ के संकेतकों (IOCs) का पता लगाना. • घटना प्रबंधन के दौरान एसओसी विश्लेषकों, थ्रेट इंटेलिजेंस टीमों, आईटी, कानूनी और बाहरी विक्रेताओं के साथ सहयोग करना. • वरिष्ठ प्रबंधन और विनियामकों (जैसे, आरबीआई, सेबी) के लिए विस्तृत घटना रिपोर्ट और डैशबोर्ड तैयार करना. • घटनोत्तर समीक्षा करना और सीखे गए सबक और निवारक नियंत्रणों के माध्यम से सुरक्षा स्थिति में सुधार लाने में योगदान देना. • आईएसओ 27001, आरबीआई साइबर सुरक्षा फ्रेमवर्क, एनआईएसटी और CERT-In सलाहों के साथ घटना प्रतिक्रिया प्रक्रियाओं को संरेखित करके अनुपालन पहलों का समर्थन करें. • घटना प्रतिक्रिया पद्धतियों, फ्रेमवर्कों और सर्वोत्तम प्रथाओं (जैसे, एनआईएसटी, आईएसओ 27001, मिटर एटीटी एवं सीके) का ज्ञान. • SIEM, EDR, फोरेंसिक टूल्स और सुरक्षा ऑर्केस्ट्रेशन और ऑटोमेशन (SOAR) प्लेटफॉर्म सहित घटना प्रतिक्रिया उपकरणों और प्रौद्योगिकियों में दक्षता. • नेटवर्किंग, ऑपरेटिंग सिस्टम (विंडोज, लिनक्स), क्लाउड प्लेटफॉर्म (जैसे, AWS, एज्योर, जीसीपी) और सुरक्षा कमजोरियों की अच्छी समझ. • स्वचालन और विश्लेषण के लिए स्क्रिप्टिंग या प्रोग्रामिंग भाषाओं (जैसे, पायथन, पॉवरशेल) का अनुभव होना अतिरिक्त योग्यता है. • उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल, जिसमें वरिष्ठ नेतृत्व सहित तकनीकी और गैर–तकनीकी हितधारकों को तकनीकी जानकारी प्रभावी ढंग से संप्रेषित करने की क्षमता शामिल है. • असाधारण विश्लेषणात्मक, समस्या–समाधान और निर्णय लेने की क्षमता, दबाव में भी गंभीर और रणनीतिक रूप से सोचने की क्षमता. • एक साथ कई घटनाओं को प्राथमिकता देने और प्रबंधित करने की क्षमता, मजबूत संगठनात्मक और समय प्रबंधन कौशल का प्रदर्शन.

पद संख्या/पद नाम	5 - उप प्रबंधक – परीक्षण इंजीनियर
मूल योग्यता (31.01.2026 तक)	**अनिवार्य:** कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री, **न्यूनतम 50% अंकों के साथ.** अथवा एम.सी.ए. अथवा कंप्यूटर विज्ञान/कंप्यूटर विज्ञान एवं इंजीनियरिंग/सूचना प्रौद्योगिकी/सॉफ्टवेयर इंजीनियरिंग/इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/एम.एससी या उपरोक्त निर्दिष्ट विषयों में समकक्ष डिग्री. (भारत सरकार द्वारा मान्यताप्राप्त/सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/संस्थान/बोर्ड से) **वरीयता:** **साइबर सुरक्षा या सूचना प्रौद्योगिकी में उच्च डिग्री को प्राथमिकता दी जाएगी.**
अन्य योग्यता (31.01.2026 तक)	**वरीयता प्रमाणपत्र:** (दिनांक 31.01.2026 को वैध) ISTQB, STQC स्टैंडर्ड मैपिंग, CTFL, CSTE, CAST, CISSP, CISM, प्रौद्योगिकी हार्डवेयर से संबंधित प्रमाणपत्रों को प्राथमिकता दी जाती है.
कार्य अनुभव (मूल योग्यता के बाद) (31.01.2026 तक)	**अनिवार्य:** न्यूनतम अनुभव: साइबर सुरक्षा/सूचना प्रौद्योगिकी क्षेत्र में योग्यता–पश्चात् 4 वर्ष का अनुभव. **वरीयता:** हार्डवेयर/सॉफ्टवेयर का परीक्षण करने और बग खोजने का अनुभव. परीक्षण योजनाओं और प्रक्रियाओं को डिजाइन करने और निष्पादित करने का अनुभव होना आवश्यक है. इसमें पायथन जैसी स्क्रिप्टिंग भाषाओं का उपयोग करके स्वचालित परीक्षण बनाना शामिल है. हार्डवेयर/सॉफ्टवेयर समस्याओं के मूल कारण का विश्लेषण करने के लिए मजबूत डिबगिंग और समस्या निवारण कौशल आवश्यक हैं. तकनीकी उत्पादों और सेवाओं का विश्लेषण. वित्त, व्यवसाय या परिचालन/प्रौद्योगिकी क्षेत्र में विश्लेषक के रूप में अनुभव. **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.** **नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो: (i) कार्य की प्रकृति, (ii) अनुभव की तिथियां और अवधि, (iii) स्तर/पद, (iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि. हालाँकि, यदि उम्मीदवार ऊपर बताए गए अनुसार अनुभव प्रमाण पत्र प्रस्तुत करने में असमर्थ है, तो अनुभव, कार्य की प्रकृति और दावा की गई अवधि को स्पष्ट रूप से दर्शाने वाला कोई भी दस्तावेज़ प्रस्तुत किया जा सकता है और बैंक के विवेक पर गुणों के आधार पर उस पर विचार किया जाएगा और बैंक का निर्णय अंतिम होगा.

विशिष्ट कौशल:	• हार्डवेयर डिज़ाइन सिद्धांतों, कंप्यूटर आर्किटेक्चर और विद्युत/इलेक्ट्रॉनिक प्रणालियों की गहन समझ. • हार्डवेयर परीक्षण पद्धतियों, परीक्षण उपकरणों और परीक्षण स्वचालन उपकरणों का अनुभव. • हार्डवेयर दोषों का निदान और निवारण करने के लिए उत्कृष्ट विश्लेषणात्मक और समस्या-समाधान कौशल. • स्पष्ट और संक्षिप्त परीक्षण योजनाएँ और रिपोर्ट तैयार करने के लिए मजबूत संचार और दस्तावेज़ीकरण कौशल. • तीव्र गति वाले, गतिशील वातावरण में काम करने और परियोजना की बदलती आवश्यकताओं के अनुकूल ढलने की क्षमता. • कंप्यूटर हार्डवेयर, हार्डवेयर परीक्षण और विश्लेषण की गहन समझ, साथ ही हार्डवेयर का मूल्यांकन करने, सिस्टम डिज़ाइन करने, अपग्रेड प्रबंधित करने और उपयोगकर्ताओं की सहायता करने के लिए मजबूत समस्या-समाधान, आलोचनात्मक सोच और संचार क्षमता. • **प्रोग्रामिंग और स्क्रिप्टिंग:** जावा या पायथन जैसी भाषाओं का ज्ञान परीक्षकों को सॉफ़्टवेयर के आर्किटेक्चर को समझने और परीक्षणों को स्वचालित करने में मदद करता है. • **ऑपरेटिंग सिस्टम:** विंडोज, macOS, लिनक्स, iOS और एंड्रॉइड जैसे विभिन्न ऑपरेटिंग सिस्टम प्लेटफॉर्म से परिचित होना संगतता परीक्षण सुनिश्चित करता है. • **टेस्ट ऑटोमेशन टूल्स:** टेस्ट केस मैनेजमेंट, डिफेक्ट ट्रैकिंग और ऑटोमेशन टूल्स में दक्षता, कार्यकुशलता के लिए अनिवार्य है. • **विश्लेषणात्मक और आलोचनात्मक सोच:** सॉफ्टवेयर का बारीकी से आकलन करने, जटिल समस्याओं को समझने और दोषों के मूल कारणों की पहचान करने की क्षमता. • **संप्रेषण:** निष्कर्षों को संप्रेषित करने, समस्याओं को स्पष्ट रूप से दस्तावेजीकृत करने और डेवलपमेंट टीमों के साथ प्रभावी ढंग से सहयोग करने के लिए मजबूत मौखिक और लिखित कौशल आवश्यक हैं. • **समस्या-समाधान:** परीक्षकों को परीक्षण प्रक्रिया के दौरान आने वाली समस्याओं का व्यवस्थित रूप से समाधान खोजने में सक्षम होना चाहिए. • **बारीकियों पर ध्यान:** सभी दोषों और उनकी सूक्ष्मताओं को सटीक रूप से पहचानने और दस्तावेज़ीकृत करने के लिए बारीकियों पर पैनी नज़र रखना महत्वपूर्ण है. • **अनुकूलनशीलता और लचीलापन:** सॉफ्टवेयर का क्षेत्र लगातार बदल रहा है, जिसके लिए परीक्षकों को अनुकूलनशील होना और नई तकनीकों और कार्यप्रणालियों को सीखने के लिए तत्पर रहना आवश्यक है. • **उपयोगकर्ता-केंद्रित मानसिकता:** उपयोगकर्ता की आवश्यकताओं को पूरा करने पर ध्यान केंद्रित करने से यह सुनिश्चित होता है कि अंतिम सॉफ्टवेयर उत्पाद उच्च गुणवत्ता वाला और उपयोगकर्ता के अनुकूल हो. • उच्च स्तर की सटीकता और बारीकियों पर ध्यान देने के साथ मजबूत विश्लेषणात्मक और समस्या-समाधान कौशल. • जटिल डेटा की व्याख्या करने, रुझानों की पहचान करने और प्रभावी समाधान प्रस्तावित करने में निपुण. • डेटा मॉडलिंग, विश्लेषण और रिपोर्टिंग के लिए माइक्रोसॉफ्ट एक्सेल में विशेषज्ञता. • बिजनेस इंटेलिजेंस (बीआई) और डेटा विज़ुअलाइज़ेशन टूल (जैसे, पावर बीआई, टैबल्यू) में दक्षता. • उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल. • विभिन्न टीमों और स्तरों पर प्रभावी ढंग से सहयोग करने और प्रभावित करने की क्षमता के साथ मजबूत हितधारक प्रबंधन कौशल. • आंतरिक और बाह्य भागीदारों के साथ मजबूत, सहयोगात्मक संबंध बनाना और बनाए रखना. • बेंचमार्किंग प्रयासों के उद्देश्य को स्पष्ट करने के लिए व्यावसायिक आवश्यकताओं और रणनीतिक उद्देश्यों को समझना.

महत्वपूर्ण बिंदु:

1. विभिन्न पदों के लिए निर्धारित शैक्षणिक योग्यता न्यूनतम है. उम्मीदवार को निर्दिष्ट तिथियों के अनुसार मूल योग्यता के बाद और प्रासंगिक पूर्णकालिक अनुभव होना चाहिए.
2. **नियोक्ता से संबंधित अनुभव प्रमाण पत्र में विशेष रूप से उल्लेख होना चाहिए कि उम्मीदवार को संबंधित क्षेत्र में अपेक्षित अनुभव है.**
3. यदि डिग्री/डिप्लोमा के प्रमाणपत्र विशेषज्ञता का क्षेत्र नहीं निर्दिष्ट करते हैं, तो उम्मीदवार को संबंधित विश्वविद्यालय/कॉलेज से विशेष रूप से विशेषज्ञता का उल्लेख करने वाला प्रमाणपत्र प्रस्तुत करना होगा.

ग. कार्य की संक्षिप्त रुपरेखा, भूमिका और दायित्व, कार्य और कार्यकलाप का विवरण:

क्र. सं.	पद	कार्य की रुपरेखा, भूमिका, उत्तरदायित्व और कार्यों के विवरण
1.	**उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ**	**कार्य प्रोफ़ाइल:** आईटी सुरक्षा विशेषज्ञ साइबर रक्षा विशेषज्ञ के रूप में कार्य करेंगे और साइबर सुरक्षा उत्कृष्टता केंद्र के अंतर्गत साइबर रक्षा केंद्र के संचालन का कार्य करेंगे. इस भूमिका में खतरे की खुफिया जानकारी, घटना प्रतिक्रिया और साइबर लचीलापन कार्यों को कवर करते हुए उन्नत साइबर रक्षा क्षमताओं का निर्माण, प्रबंधन और संचालन शामिल है. वे विनियामक और संगठनात्मक आवश्यकताओं के अनुपालन को सुनिश्चित करते हुए साइबर खतरों की निगरानी, पता लगाने, विश्लेषण करने और प्रतिक्रिया देने के लिए जिम्मेदार होंगे. **मुख्य दायित्व क्षेत्र (केआरए):** **जमीनी क्रियान्वयन:** • साइबर विश्लेषकों, थ्रेट हंटर्स, घटना प्रतिक्रियाकर्ताओं और सुरक्षा इंजीनियरों की टीम के साथ काम करना. • सरकारी एजेंसियों, विनियामकों, उद्योग भागीदारों और शिक्षाविदों के साथ सहयोग को बढ़ावा देना. **परिचालन प्रबंधन** • सुरक्षा घटनाओं का समय पर पता लगाना, उनका वर्गीकरण करना और प्रतिक्रिया देना सुनिश्चित करना. • घटना प्रतिक्रिया और साइबर संकट प्रबंधन के लिए कार्ययोजना विकसित करना और उसे कार्यान्वित करना. • थ्रेट इंटेलिजेस जीवनचक्र का प्रबंधन करना: संग्रह, विश्लेषण, प्रसार और कार्रवाई. • सुरक्षा संबंधी कमियों के प्रबंधन और सक्रिय थ्रेट हंटिंग पहलों की निगरानी करना. • रेड टीम/ब्लू टीम अभ्यास, सिमुलेशन और मॉक ड्रिल आयोजित करके साइबर सुरक्षा को बनाए रखना. **अभिशासन एवं अनुपालन** • राष्ट्रीय और अंतर्राष्ट्रीय साइबर सुरक्षा मानकों (आईएसओ 27001, एनआईएसटी, CERT-In दिशानिर्देश, आरबीआई/सेबी/MeitY सलाह) की अनुरूपता सुनिश्चित करें. • नेतृत्व और विनियामक निकायों के लिए आवधिक जोखिम, खतरे और घटना रिपोर्ट तैयार करना. • ऑडिट, अनुपालन आकलन और साइबर सुरक्षा परिपक्वता मूल्यांकन में सहयोग करना. **क्षमता निर्माण एवं नवाचार** • अनुसंधान, फ्रेमवर्क और सर्वोत्तम प्रथाओं के माध्यम से CoE के ज्ञान भंडार में योगदान देना. • उभरती साइबर रक्षा प्रौद्योगिकियों (सुरक्षा में एआई/एमएल, SOAR, SIEM², XDR, क्लाउड सुरक्षा) पर टीम के सदस्यों को मार्गदर्शन और कौशल विकास प्रदान करना. • स्टार्टअप, अकादमिक संस्थानों और वैश्विक साइबर रक्षा मंचों के साथ जुड़कर नवाचार को बढ़ावा दें.

2.	उप प्रबंधक – उभरती प्रौद्योगिकी	**कार्य प्रोफ़ाइल:** यह संगठन की सुरक्षा स्थिति को विकसित होते साइबर खतरों से बचाने के लिए नई रणनीतियों, प्रौद्योगिकियों और कार्यप्रणालियों की पहचान, विकास और कार्यान्वयन करता है. वे साइबर सुरक्षा पहलों का नेतृत्व करने, नए समाधानों का मूल्यांकन करने और यह सुनिश्चित करने के लिए जिम्मेदार हैं कि एक संगठन गतिशील खतरे के परिदृश्य में लचीला और सुरक्षित बना रहे, जिसके लिए तकनीकी विशेषज्ञता और खतरे के प्रबंधन के लिए नए दृष्टिकोण बनाने के लिए एक नवोन्मेषी मानसिकता की आवश्यकता होती है. यह व्यवसाय की आवश्यकताओं को प्रौद्योगिकी या साइबर समाधानों से जोड़ने में महत्वपूर्ण भूमिका निभाएगा. विश्लेषक व्यावसायिक इकाइयों, डेवलपर्स और परियोजना टीमों के साथ मिलकर काम करता है ताकि यह सुनिश्चित किया जा सके कि प्रौद्योगिकी/साइबर पहलें संगठनात्मक लक्ष्यों के अनुरूप हों. साइबर सुरक्षा क्षेत्र में नवाचार और व्यावहारिक अनुसंधान को बढ़ावा देना. उभरती सुरक्षा प्रौद्योगिकियों का मूल्यांकन करना और बैंकिंग परिवेश में उनकी प्रयोज्यता का आकलन करना. उन्नत साइबर सुरक्षा समाधानों के लिए प्रूफ–ऑफ–कॉन्सेप्ट (PoCs) और पायलट परियोजनाएं तैयार करना. नवीन समाधानों की खोज, सत्यापन और अनुकूलन के लिए स्टार्ट–अप, इनक्यूबेटर और अनुसंधान संस्थानों के साथ जुड़ना. साइबर सुरक्षा नवाचार के लिए आंतरिक उपकरण, फ्रेमवर्क और कार्यप्रणालियों को डिजाइन करने में सहायता करना. संगठनों को सोच–विचार कर निर्णय लेने में मदद करने के लिए डेटा एकत्र करने, विश्लेषण करने और उसकी व्याख्या करने के लिए जिम्मेदार. इस भूमिका के लिए मजबूत विश्लेषणात्मक और संप्रेषण कौशल, बारीकियों पर ध्यान देने की क्षमता और जटिल डेटा को उपयोगी अंतर्दृष्टि में बदलने की क्षमता आवश्यक है. इस भूमिका में अनुसंधान पहल करना, साइबर सुरक्षा में नवाचार को बढ़ावा देना और यह सुनिश्चित करना शामिल है कि संगठन की साइबर सुरक्षा मजबूत और प्रभावी हो. **मुख्य दायित्व क्षेत्र (केआरए):** **प्रौद्योगिकी विश्लेषण एवं विकास:** • व्यावसायिक आवश्यकताओं के लिए उपयुक्तता और संभावित प्रभाव का निर्धारण करने हेतु नई और मौजूदा प्रौद्योगिकियों का मूल्यांकन करना. • डिजिटल परिदृश्य में नए साइबर खतरों और कमजोरियों का पूर्वानुमान लगाकर नवीनतम तकनीकों से अवगत रहना. • प्रौद्योगिकी/साइबर समाधानों के लिए व्यवहार्यता अध्ययन और लागत–लाभ विश्लेषण करना. • साइबर सुरक्षा को मजबूत करने के लिए नवीन तकनीकी समाधानों और ढाँचों पर शोध, डिज़ाइन और कार्यान्वयन करना. • नेटवर्क, सिस्टम और डेटा की सुरक्षा के लिए अत्याधुनिक प्रौद्योगिकियों और प्रक्रियाओं को लागू करने वाली परियोजनाओं का नेतृत्व करना. **व्यवसाय और सिस्टम विश्लेषण:** • तकनीकी और व्यावसायिक आवश्यकताओं को एकत्रित करने और उनका विश्लेषण करने के लिए व्यावसायिक हितधारकों के साथ सहयोग करना. • व्यावसायिक आवश्यकताओं को कार्यात्मक और तकनीकी विशिष्टताओं में रूपांतरित करना. • व्यवसाय प्रक्रिया पुनर्विन्यास और डिजिटल परिवर्तन पहलों में सहयोग प्रदान करना. **समाधान डिज़ाइन और कार्यान्वयन सहायता:** • सिस्टम आर्किटेक्चर, डेटा प्रवाह और एकीकरण बिंदुओं को डिज़ाइन करना. • कार्यान्वयन के दौरान सॉफ़्टवेयर डेवलपर्स, आईटी इंजीनियरों और वेंडरों के साथ काम करना. • यह सुनिश्चित करना कि समाधान व्यावसायिक, तकनीकी और अनुपालन अपेक्षाओं को पूरा करते हों. **तकनीकी दस्तावेज़ीकरण और रिपोर्टिंग:** • सिस्टम और प्रक्रिया दस्तावेज़ीकरण, उपयोगकर्ता मार्गदर्शिकाएँ और तकनीकी मैनुअल तैयार करना. • प्रबंधन हितधारकों को तकनीकी रिपोर्ट और डैशबोर्ड प्रदान करना. • निष्कर्षों, प्रौद्योगिकी विकल्पों और अनुशंसाओं को स्पष्ट और व्यवसाय अनुकूल तरीके से प्रस्तुत करना. • साइबर सुरक्षा नवाचार के लिए एक सहयोगात्मक पारिस्थितिकी तंत्र को बढ़ावा देने के लिए अनुसंधान संस्थानों और उद्योग भागीदारों सहित आंतरिक और बाहरी हितधारकों के साथ जुड़ना. **योजना बनाना:** साइबर सुरक्षा अनुसंधान और विकास के लिए केंद्र की रणनीतिक विजन और रोडमैप तैयार करना और उसे लागू करना. **अनुसंधान और नवाचार:** उभरते साइबर खतरों की पहचान करने और उन्हें कम करने, नई सुरक्षा प्रौद्योगिकियों को विकसित करने और मौजूदा सुरक्षा प्रोटोकॉल को बेहतर बनाने पर केंद्रित अनुसंधान परियोजनाओं की देखरेख करना. **सहयोग और साझेदारी:** साइबर सुरक्षा ज्ञान और क्षमताओं को आगे बढ़ाने के लिए आंतरिक टीमों, बाहरी अनुसंधान संस्थानों और उद्योग भागीदारों के साथ मिलकर काम करना. **ज्ञान साझा करना:** शोध निष्कर्षों और सर्वोत्तम प्रथाओं को पूरे संगठन में और संभाव्यत: व्यापक साइबर सुरक्षा समुदाय तक प्रसारित करना. **खतरों से आगे रहना:** संगठन की सुरक्षा सुनिश्चित करने के लिए नवीनतम साइबर सुरक्षा प्रवृत्तियों, खतरों और प्रौद्योगिकियों की जानकारी रखना. **साइबर सुरक्षा अनुसंधान और इंटेलिजेंस जानकारी:** उभरते साइबर सुरक्षा खतरों, कमजोरियों, उपकरणों, प्रौद्योगिकियों और सर्वोत्तम प्रथाओं पर निरंतर अनुसंधान करना. शैक्षणिक, सरकारी और उद्योग स्रोतों से साइबर सुरक्षा विकास की निगरानी करना. अनुसंधान निष्कर्षों को आंतरिक हितधारकों के लिए उपयोगी जानकारियों में संकलित करना. साइबर सुरक्षा पहलों के लिए रणनीतिक योजना, क्षमता विकास और निवेश निर्णयों का समर्थन करने हेतु अनुसंधान–आधारित अंतर्दृष्टि प्रदान करना.

3.	**उप प्रबंधक – साइबर सुरक्षा विश्लेषक**	**कार्य प्रोफ़ाइल:** साइबर सुरक्षा उत्कृष्टता केंद्र में कार्यरत एथिकल हैकिंग और रेड टीम विश्लेषक, संगठन के बुनियादी ढांचे, अनुप्रयोगों, मोबाइल ऐप्स और प्रक्रियाओं में सुरक्षा कमजोरियों की पहचान करने, उनका लाभ उठाने और कार्रवाई योग्य जानकारी प्रदान करने के लिए जिम्मेदार होंगे. यह भूमिका वास्तविक हमलों का अनुरूपण करेगी, उन्नत भेदन परीक्षण करेगी और संगठन की समग्र सुरक्षा स्थिति को मजबूत करने में योगदान देगी. विशेषज्ञ उत्कृष्टता केंद्र की रेड टीमिंग पद्धतियों और क्षमताओं को विकसित करने और परिष्कृत करने, तथा सुरक्षा जागरूकता और लचीलेपन की संस्कृति को बढ़ावा देने में महत्वपूर्ण भूमिका निभाएंगे. **मुख्य दायित्व क्षेत्र (केआरए):** **रेड टीमिंग और विरोधी सिमुलेशन:** रेड टीमिंग परीक्षण तकनीकों और मिट्रे एटीटी एवं सीके फ्रेमवर्क का उपयोग करते हुए, उन्नत हमलावरों की नकल करने वाले कस्टम एक्सप्लॉइट्स और तकनीकों का उपयोग करके, वास्तविक हमले के परिदृश्यों के विरुद्ध सुरक्षा नियंत्रणों का परीक्षण करने के लिए रेड टीम गतिविधियों की योजना बनाना और उन्हें क्रियान्वित करना. **पेनेट्रेशन टेंस्टिंग:** जटिल कमजोरियों की पहचान करने के लिए स्वचालित और मैन्युअल विधियों का उपयोग करके नेटवर्क, अनुप्रयोगों, मोबाइल ऐप और सिस्टम का गहन पेनेट्रेशन टेंस्टिंग और एक्सप्लॉइट करना. **सुरक्षा भेद्यता अनुसंधान और एक्सप्लॉइट विकास:** खतरों पर अद्यतन जानकारी रखना और सुरक्षा भेद्यताओं का परीक्षण करने और शून्य–दिन की भेद्यताओं की पहचान करने के लिए अनुकूलित एक्सप्लॉइट विकसित करना. **सुरक्षित कोड समीक्षा:** हमलावर के दृष्टिकोण से कोड की सुरक्षा भेद्यताओं की समीक्षा करना. **बग बाउंटी:** उनके सॉफ़्टवेयर या सिस्टम में सुरक्षा भेद्यताओं को खोजना और रिपोर्ट करना, जिससे दुर्भावनापूर्ण तत्वों द्वारा उनका एक्सप्लॉइट करने से पहले खामियों की पहचान करने और उन्हें ठीक करने में मदद मिल सके. **सुरक्षा भेद्यता प्रबंधन:** सुरक्षा खामियों दूर करने के उपायों की प्रभावशीलता का सत्यापन और प्रमाणीकरण करना. **सहयोग एवं संचार:** सुरक्षा में सुधार के लिए अन्य टीमों के साथ मिलकर काम करना और निष्कर्षों को स्पष्ट रूप से दस्तावेजीकृत और प्रस्तुत करना. **सुरक्षा उपकरण एवं स्वचालन:** आक्रामक सुरक्षा उपकरणों और प्रक्रियाओं का मूल्यांकन और स्वचालन करना. **निरंतर सीखना एवं अनुसंधान:** सुरक्षा प्रवृत्तियों से अवगत रहना और साइबर सुरक्षा समुदायों में सक्रिय रूप से भाग लेना.
4.	**उप प्रबंधक – घटना प्रबंधन और फोरेंसिक**	**कार्य प्रोफ़ाइल:** यह एक महत्वपूर्ण भूमिका है, जिसमें संपूर्ण घटना प्रतिक्रिया चक्र की निगरानी करना, संगठन भर में साइबर हमलों और सुरक्षा उल्लंघनों से त्वरित पहचान, रोकथाम, उन्मूलन, रैंसमवेयर और रिकवरी सुनिश्चित करना शामिल है. आप समर्पित आईआर विशेषज्ञों की एक टीम का नेतृत्व, मार्गदर्शन और सशक्तिकरण करेंगे, घटना प्रतिक्रिया प्रक्रियाओं, ढांचे, एसओपी और प्लेबुक को परिभाषित और परिष्कृत करेंगे और उभरते साइबर खतरों के खिलाफ तैयारी, निरंतर सुधार और सहयोगात्मक रक्षा की संस्कृति को बढ़ावा देंगे. उत्कृष्टता केंद्र (सीओई) में, वह सुरक्षा घटनाओं की जांच करने, मैलवेयर का विश्लेषण करने और संगठन की सुरक्षा स्थिति में सुधार के लिए रणनीतियां विकसित करने के लिए जिम्मेदार होगा. इस भूमिका के लिए मैलवेयर विश्लेषण और डिजिटल फोरेंसिक में मजबूत तकनीकी विशेषज्ञता आवश्यक है. **मुख्य दायित्व क्षेत्र (केआरए):** • संगठन के भीतर साइबर घटनाओं, धोखाधड़ी, डेटा लीक और नीति उल्लंघनों से संबंधित संपूर्ण फोरेंसिक जांच करना. • एंडपॉइंट डिवाइस, सर्वर, क्लाउड प्लेटफॉर्म और मोबाइल डिवाइस सहित विभिन्न प्रणालियों में डिजिटल साक्ष्यों का अधिग्रहण, संरक्षण और विश्लेषण करना. • कोर बैंकिंग और लेनदेन डेटा का उपयोग करके वित्तीय धोखाधड़ी, आंतरिक खतरों और भुगतान प्रणालियों में अनियमितताओं की जांच करना. • आंतरिक समीक्षाओं, कानूनी कार्यवाही और विनियामक निकायों (जैसे, आरबीआई, सेबी) के लिए विस्तृत फोरेंसिक रिपोर्ट, समय–सीमा और साक्ष्य तैयार करना. • जांच में सहयोग करने और विनियामक अनुपालन सुनिश्चित करने के लिए आंतरिक टीमों (कानूनी, अनुपालन, जोखिम और आईटी सुरक्षा) के साथ मिलकर काम करना. • साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने में विशेषज्ञ सहायता प्रदान करना, जिसमें मूल कारण विश्लेषण और सुधारात्मक कार्रवाई के लिए सिफारिशें शामिल हों. • यह सुनिश्चित करना कि सभी फोरेंसिक जांच भारतीय साइबर कानूनों और साक्ष्य प्रबंधन की सर्वोत्तम प्रथाओं के अनुसार की जाएं. • फोरेंसिक टूलसेट को बनाए रखना और उभरते खतरों, तकनीकों और विनियामक दिशानिर्देशों की जानकारी रखना. • डिजिटल फोरेंसिक और साइबर जांच का संचालन करना, जिसमें विभिन्न घटनाओं की निगरानी करना, फोरेंसिक प्रक्रियाओं और साक्ष्य प्रबंधन का निर्देशन करना, कानूनी और कानून प्रवर्तन एजेंसियों के साथ समन्वय करना और उन्नत खतरों की जांच का नेतृत्व करना शामिल है. • मैलवेयर विश्लेषण और खतरे की खुफिया जानकारी जुटाना, जिसमें विश्लेषण और रिवर्स इंजीनियरिंग की निगरानी करना, खतरे की खुफिया जानकारी टीमों के साथ सहयोग करना और घटना प्रतिक्रिया प्रोटोकॉल को परिष्कृत करना शामिल है. • फोरेंसिक विश्लेषकों के प्रबंधन और मार्गदर्शन पर ध्यान केंद्रित करना, तकनीकी मार्गदर्शन प्रदान करना और प्रदर्शन समीक्षा करना. • घटना प्रतिक्रिया और सुरक्षा स्थिति में सुधार करना, जिसमें एक एस्केलेशन पॉइंट के रूप में कार्य करना, विश्लेषण अपडेट की निगरानी करना, तत्परता पहलों का समर्थन करना, विक्रेताओं के साथ समन्वय करना और विभिन्न कार्यों में विभाग का प्रतिनिधित्व करना शामिल है. • दस्तावेज़ीकरण और रिपोर्टिंग, जिसमें विस्तृत रिपोर्ट सुनिश्चित करना और कानूनी और लेखापरीक्षा उद्देश्यों के लिए रिकॉर्ड बनाए रखना शामिल है. • एंडपॉइंट, सर्वर, मोबाइल डिवाइस और क्लाउड प्लेटफॉर्म पर संपूर्ण डिजिटल फोरेंसिक का संचालन करना. • जांच में सहायता के लिए फोरेंसिक इमेजिंग, लॉग विश्लेषण और आर्टिफैक्ट एक्सट्रैक्शन करना. • आंतरिक हितधारकों, कानूनी और विनियामक निकायों के लिए फोरेंसिक रिपोर्ट प्रदान करना. • दुर्भावनापूर्ण कोड, स्क्रिप्ट और एक्सप्लॉइट्स का विश्लेषण और रिवर्स इंजीनियरिंग करना. • मैलवेयर के व्यवहार को समझने के लिए सैंडबॉक्सिंग, स्टैटिक/डायनेमिक विश्लेषण और डिबगिंग टूल का उपयोग करना. • घटना प्रतिक्रिया कार्यों के दौरान फोरेंसिक और मैलवेयर विश्लेषण विशेषज्ञता प्रदान करना. • मैलवेयर संबंधी जानकारियाँ साझा करके खतरे की खुफिया जानकारी में योगदान देना. • टेबल–टॉप अभ्यास और खतरे के सिमुलेशन में भाग लेना.

घटना प्रतिक्रिया एवं प्रबंधन:

- घटना प्रतिक्रिया टीम का संचालन और प्रबंधन करना, जिसमें घटना प्रतिक्रिया जीवनचक्र के सभी चरण शामिल हैं, जैसे कि पहचान, विश्लेषण, रोकथाम, उन्मूलन, पुनर्प्राप्ति और घटना के बाद की गतिविधियाँ.
- महत्वपूर्ण घटनाओं के दौरान एकीकृत और प्रभावी प्रतिक्रिया सुनिश्चित करने के लिए आईटी संचालन, सुरक्षा संचालन, कानूनी और संचार सहित विभिन्न विभागों की टीमों के बीच घटना प्रतिक्रिया प्रयासों का समन्वय करना.
- उच्च प्राथमिकता वाली घटनाओं के लिए प्राथमिक संपर्क बिंदु और समाधानकर्ता के रूप में कार्य करना, घटना प्रतिक्रिया टीम और हितधारकों को मार्गदर्शन और निर्णायक नेतृत्व प्रदान करना.

रणनीति, प्रक्रिया एवं प्लेबुक विकास:

- संगठन की घटना प्रतिक्रिया रणनीति, प्रक्रियाओं, कार्यविधियों और प्लेबुक को विकसित करना, लागू करना और लगातार परिष्कृत करना, यह सुनिश्चित करते हुए कि वे उद्योग की सर्वोत्तम प्रथाओं (जैसे, एनआईएसटी, आईएसओ 27001) और विनियामक अपेक्षाओं के अनुरूप हों.
- विभिन्न प्रकार की सुरक्षा घटनाओं और संगठनात्मक संपत्तियों के अनुरूप व्यापक घटना प्रतिक्रिया योजनाओं, प्रक्रियाओं और रनबुक के विकास और रखरखाव को बढ़ावा देना.
- घटना का पता लगाने, विश्लेषण करने और प्रतिक्रिया देने की कार्यप्रवाह को सुव्यवस्थित करने के लिए घटना प्रबंधन प्लेटफॉर्म और उपकरणों (जैसे SIEM, EDR, SOAR) को लागू करना और उनका उपयोग करना.

जांच एवं फोरेंसिक विश्लेषण:

- सुरक्षा संबंधी घटनाओं के मूल कारण, दायरे और प्रभाव का पता लगाने के लिए गहन जांच और फोरेंसिक विश्लेषण की निगरानी करना. कानूनी और फोरेंसिक मानकों का पालन करते हुए डिजिटल साक्ष्यों का उचित संग्रह, संरक्षण और विश्लेषण सुनिश्चित करना.
- आवश्यकता पड़ने पर कानूनी सलाहकारों और कानून प्रवर्तन एजेंसियों के साथ सहयोग करना, कानूनी आवश्यकताओं और रिपोर्टिंग दायित्वों का अनुपालन सुनिश्चित करना.

टीम विकास एवं मार्गदर्शन:

- घटना प्रतिक्रिया विशेषज्ञों की टीम के साथ काम करना, उच्च प्रदर्शन, सहयोगात्मक और शिक्षण केंद्रित वातावरण को बढ़ावा देना.
- घटना प्रतिक्रिया टीम के कौशल, ज्ञान और तैयारी को बढ़ाने के लिए प्रशिक्षण कार्यक्रम, कार्यशालाएं और अभ्यास सत्र विकसित करना और प्रदान करना.
- कार्य-निष्पादन समीक्षा करना, रचनात्मक प्रतिक्रिया देना और टीम सदस्यों के निरंतर व्यावसायिक विकास और कॅरियर विकास में सहयोग करना.

सुधार एवं रिपोर्टिंग:

- घटना प्रतिक्रिया प्रक्रियाओं, प्रौद्योगिकियों और टीम क्षमताओं में सुधार के क्षेत्रों की पहचान करने के लिए घटनोत्तर समीक्षा (पीआईआर) और सीखे गए सबक सत्र आयोजित करना.
- वरिष्ठ प्रबंधन और हितधारकों को घटना संबंधी रिपोर्ट और संक्षिप्त जानकारी तैयार करके प्रस्तुत करना, जिसमें घटना की प्रवृत्ति, जोखिम और निवारण एवं रोकथाम के लिए सिफारिशें शामिल हों.

5. उप प्रबंधक – परीक्षण इंजीनियर

<u>कार्य प्रोफ़ाइल:</u>

इस भूमिका में आंतरिक और बाह्य परिचालन एवं कार्य-निष्पादन संबंधी कमियों की पहचान करने के लिए डेटा का विश्लेषण करना, निरंतर सुधार को बढ़ावा देना और रणनीतिक निर्णयों के लिए उपयोगी अंतर्दृष्टि प्रदान करना शामिल है. इसके लिए अक्सर हितधारकों के साथ सहयोग करने और उद्योग की सर्वोत्तम प्रथाओं के अनुरूप दक्षता एवं प्रदर्शन में सुधार लाने के लिए मजबूत विश्लेषणात्मक, संचार और परियोजना प्रबंधन कौशल की आवश्यकता होती है.

यह भूमिका उत्पाद जारी होने से पहले हार्डवेयर घटकों और प्रणालियों का मूल्यांकन, परीक्षण और सत्यापन करने के लिए जिम्मेदार है ताकि यह सुनिश्चित किया जा सके कि वे प्रदर्शन, विश्वसनीयता और गुणवत्ता मानकों को पूरा करते हैं. यह भूमिका उत्पाद जीवनचक्र के दौरान समस्याओं की पहचान और निवारण के लिए तकनीकी विशेषज्ञता को मजबूत विश्लेषणात्मक और समस्या-समाधान कौशल के साथ जोड़ती है. इस भूमिका में आवश्यकताओं का विश्लेषण करना, परीक्षण योजनाओं और मामलों को डिजाइन करना, परीक्षण वातावरण स्थापित करना, विभिन्न प्रकार के परीक्षण (कार्यात्मक, प्रदर्शन, सुरक्षा) निष्पादित करना, दोषों को लॉग करना और सॉफ्टवेयर की गुणवत्ता और विश्वसनीयता सुनिश्चित करने के लिए हितधारकों को परिणाम संप्रेषित करना शामिल है.

प्रमुख जिम्मेदारियों में डेवलपर्स के साथ सहयोग करना, प्लेटफार्मों पर कार्यक्षमता का सत्यापन करना, उपयोगिता संबंधी समस्याओं की पहचान करना और उत्पाद में सुधार के लिए सुझाव देने हेतु डिजाइन समीक्षाओं में भाग लेना शामिल है.

<u>मुख्य दायित्व क्षेत्र (केआरए):</u>

- कंप्यूटर क्षमताओं, विषयवस्तु, प्रोग्रामिंग भाषा और तर्क के ज्ञान का उपयोग करते हुए आवश्यकताओं का विश्लेषण करके, कार्यप्रवाह चार्ट और आरेख तैयार करके परियोजना की आवश्यकताओं को प्रोग्रामिंग क्रम में व्यवस्थित करना.
- सभी सॉफ़्टवेयर सिस्टम, टूल्स और एप्लिकेशन का रखरखाव, प्रबंधन और संशोधन करना.
- कार्यात्मक विशिष्टताओं का विकास और विश्लेषण करना.
- अंतिम उपयोगकर्ताओं और सॉफ़्टवेयर सलाहकारों के बीच संपर्क सूत्र के रूप में कार्य करना.
- व्यावसायिक आवश्यकताओं और उद्देश्यों से संबंधित जटिल समस्याओं का समाधान करना.
- एप्लिकेशन और टूल्स को स्थापित करने और उनका विश्लेषण करने में सॉफ़्टवेयर पेशेवरों के साथ समन्वय और सहयोग करना.
- परीक्षण प्रक्रियाओं, प्रोग्रामिंग और दस्तावेज़ीकरण का विकास, विश्लेषण और कार्यान्वयन करना.
- अन्य सॉफ़्टवेयर विश्लेषकों को प्रशिक्षित और विकसित करना.
- प्रदर्शन को बेहतर बनाने के लिए मौजूदा सिस्टम में संशोधन और परिवर्तनों का विश्लेषण, डिज़ाइन और विकास करना.
- सॉफ़्टवेयर बेंचमार्किंग: किसी सॉफ़्टवेयर के प्रदर्शन, जैसे उसकी गति, स्थिरता और संसाधन उपयोग, को स्थापित मानकों या प्रतिस्पर्धियों के विरुद्ध मापना ताकि सुधार के क्षेत्रों की पहचान की जा सके. इसमें किसी सॉफ़्टवेयर एप्लिकेशन के प्रदर्शन की तुलना परिभाषित लक्ष्यों या उद्योग औसत से करने के लिए मात्रात्मक मेट्रिक्स और परीक्षण वातावरण स्थापित करना शामिल है, जो अंततः अनुकूलन का मार्गदर्शन करता है और यह सुनिश्चित करता है कि रिलीज़ से पहले यह वांछित गुणवत्ता मानकों को पूरा करता है.

बेंचमार्किंग:

- सीपीयू, जीपीयू, मेमोरी और स्टोरेज डिवाइस जैसे अलग-अलग हार्डवेयर घटकों और मॉड्यूल का मूल्यांकन करना.
- इस प्रकार के परीक्षण से वास्तविक शक्ति और दक्षता का मापन होता है, जिससे विभिन्न परिस्थितियों में प्रत्येक घटक के प्रदर्शन की जानकारी मिलती है.

हार्डवेयर विकास और संस्थापना:

- हार्डवेयर अपग्रेड या नए हार्डवेयर खरीदने की अनुशंसा करने के लिए संगठन की आवश्यकताओं का आकलन करना.
- कंपनी के मानकों के अनुरूप और मौजूदा सिस्टम के साथ संगत हार्डवेयर स्थापित और कॉन्फ़िगर करना.
- कंपनी के मानकों के अनुरूप और मौजूदा सिस्टम के साथ संगत हार्डवेयर सुनिश्चित करना.

परीक्षण योजना और डिज़ाइन:

- हार्डवेयर डिज़ाइन विनिर्देशों और ग्राहक आवश्यकताओं के आधार पर व्यापक परीक्षण योजनाएँ, परीक्षण मामले और परीक्षण रणनीतियाँ बनाना.
- हार्डवेयर प्रदर्शन का परीक्षण और मूल्यांकन करने के सबसे सामान्य और सुविधाजनक तरीकों में से एक बेंचमार्किंग टूल का उपयोग करना है.
- बेंचमार्किंग टूल सॉफ़्टवेयर एप्लिकेशन हैं जो आपके हार्डवेयर पर मानकीकृत परीक्षण चलाते हैं और ऐसे स्कोर और मेट्रिक्स उत्पन्न करते हैं जो इसकी क्षमताओं को दर्शाते हैं.

बेंचमार्किंग और प्रदर्शन विश्लेषण:

- प्रदर्शन की तुलना के लिए प्रासंगिक आंतरिक मेट्रिक्स और बाहरी बेंचमार्क की पहचान करना.
- उद्योग के समकक्षों, प्रतिस्पर्धियों या वैश्विक मानकों के विरुद्ध तुलनात्मक विश्लेषण करना.
- प्रदर्शन में कमियों का मूल्यांकन करें और सुधार के अवसरों की अनुशंसा करना.

निरंतर सुधार:

डेटा अंतर्दृष्टि पर आधारित समाधानों को लागू करके प्रदर्शन में सुधार और परिणामों को अनुकूलित करने के लिए पहल करना.

हितधारक सहयोग:

डेटा एकत्र करने, अंतर्दृष्टि साझा करने और सुधार रणनीतियों पर सहमति बनाने के लिए क्रॉस-फंक्शनल टीमों (जैसे, मार्केटिंग, सेल्स, परिचालन, वित्त) के साथ मिलकर काम करना.

रणनीतिक अंतर्दृष्टि:

रणनीतिक योजना, विकास पहलों और परिचालन दक्षता को सूचित करने के लिए प्रबंधन को कार्रवाई योग्य अनुशंसाएँ प्रदान करना.

प्रक्रिया अनुकूलन:

निर्धारित लक्ष्यों और उपयोगकर्ता आवश्यकताओं के आधार पर प्रदर्शन मापने के लिए फ्रेमवर्क के विकास और कार्यान्वयन में सहयोग करना.

डेटा प्रबंधन और गुणवत्ता:

- बेंचमार्किंग के लिए उपयोग किए जाने वाले डेटा की उपलब्धता और गुणवत्ता सुनिश्चित करना, विसंगतियों को दूर करने के लिए डेटा टीमों के साथ मिलकर काम करना.
- सटीकता और अखंडता सुनिश्चित करने के लिए डेटा और रिपोर्टों पर गुणवत्ता आश्वासन लागू करना.
- बेंचमार्किंग प्रक्रियाओं, कार्यप्रणालियों और पहचानी गई समस्याओं का दस्तावेजीकरण करना.

प्रक्रिया सुधार और रणनीति:

- प्रक्रिया अनुकूलन और परिचालन दक्षता में सुधार के लिए रणनीतिक पहलों की अनुशंसा करने हेतु बेंचमार्किंग से प्राप्त जानकारियों का लाभ उठाना.
- समग्र बेंचमार्किंग रणनीति और कार्यप्रणाली को विकसित करने और परिष्कृत करने में सीओई का सहयोग करना.
- बेंचमार्किंग परिणामों पर चर्चा करने और कार्य योजनाओं को आगे बढ़ाने के लिए कार्यशालाओं और बैठकों का आयोजन करना.

रिपोर्टिंग और अंतर्दृष्टि सृजन:

- निष्कर्षों और प्रमुख प्रदर्शन संकेतकों (KPIs) को संप्रेषित करने के लिए डैशबोर्ड, रिपोर्ट और प्रस्तुतियाँ विकसित करना.
- जटिल डेटा को हितधारकों और नेतृत्व के लिए स्पष्ट अंतर्दृष्टि और विवरणों में परिवर्तित करना.
- प्रवृत्तियों पर नज़र रखना और प्रतिस्पर्धात्मक लाभ या जोखिम वाले क्षेत्रों की पहचान करना.

टिप्पणी: वास्तविक केआरए कार्यग्रहण करने पर सौंपा जाएगा. ऊपर वर्णित भूमिकाएं/दायित्व/कार्य रूपरेखा उदाहरण स्वरुप में हैं. ऊपर उल्लिखित दायित्वों के अलावा, अन्य भूमिकाएं/ जिम्मेदारियां/ गतिविधियां/ मुख्य पारस्परिक क्रियाएं/ गतिविधियाँ बैंक द्वारा समय-समय पर आवश्यकता के आधार पर सौंपी जा सकती हैं.

नियमित पदों पर चयनित उम्मीदवार एसबीआई के कर्मचारियों पर लागू सेवा नियमों द्वारा शासित होंगे.

घ. पारिश्रमिक/ सुझाया गया तैनाती स्थान:

क्र. सं.	पद का नाम	श्रेणी	वेतनमान	सुझाया गया तैनाती स्थान
1.	उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ	एमएमजीएस-II	**मूल वेतन: 64820-2340/1-67160-2680/10-93960** समय-समय पर लागू नियमों के अनुसार महँगाई भत्ता, मकान किराया भत्ता, नगर प्रतिपूरक भत्ता, पीएफ, अंशदायी पेंशन फंड यानी एनपीएस, एलएफसी, चिकित्सा सुविधा, अवकाश आदि और बैंक की वेतन संरचना के अनुसार वेतन और भत्ते के लिए पात्र.	**मुंबई या किसी भी प्रशासनिक आवश्यकता के मामले में भारत में कहीं भी.**
2.	उप प्रबंधक – उभरती प्रौद्योगिकी			
3.	उप प्रबंधक – साइबर सुरक्षा विश्लेषक			
4.	उप प्रबंधक – घटना प्रबंधन और फोरेंसिक			
5.	उप प्रबंधक – परीक्षण इंजीनियर			

ङ. चयन प्रक्रिया: चयन शॉर्टलिस्टिंग और साक्षात्कार के आधार पर होगा.

- ❖ **शॉर्टलिस्टिंग: न्यूनतम योग्यता और अनुभव होने मात्र से उम्मीदवार को साक्षात्कार के लिए बुलाए जाने का कोई अधिकार नहीं होगा.** बैंक द्वारा गठित शॉर्टलिस्टिंग समिति शॉर्टलिस्टिंग मानदंड निर्धारित करेगी और उसके पश्चात् बैंक द्वारा लिये गये निर्णय के अनुसार पर्याप्त संख्या में उम्मीदवार शॉर्टलिस्ट कर साक्षात्कार के लिए बुलाए जाएंगे. बातचीत के लिए उम्मीदवारों को बुलाए जाने का बैंक का निर्णय अंतिम होगा. **इस संबंध में किसी भी पत्राचार पर विचार नहीं किया जाएगा.**
- ❖ **साक्षात्कार:** साक्षात्कार 100 अंकों का होगा. साक्षात्कार में अर्हक अंक बैंक द्वारा तय किए जाएंगे. इस संबंध में किसी भी पत्राचार पर विचार नहीं किया जाएगा.
- ❖ **मेरिट सूची:** चयन के लिए मेरिट सूची केवल साक्षात्कार में प्राप्त अंकों के आधार पर अवरोही क्रम में तैयार की जाएगी. एक से अधिक उम्मीदवारों द्वारा निर्दिष्ट अंक प्राप्त करने पर (निर्दिष्ट सीमा पर एक समान अंक होने पर), ऐसे उम्मीदवारों को मेरिट सूची में उनकी आयु के आधार पर अवरोही क्रम में रैंक की जाएगी.

च. साक्षात्कार के लिए कॉल लेटर:

बातचीत के लिए सूचना/ कॉल लेटर बैंक की वेबसाइट पर अपलोड किया जाएगा या ईमेल द्वारा भेजा जाएगा, जैसा भी बैंक द्वारा तय किया जाएगा. **कोई हार्ड कॉपी नहीं भेजी जाएगी.**

छ. आवेदन कैसे करें:

उम्मीदवारों की **वैध ईमेल आईडी** हो जिसे परिणाम घोषित होने तक एक्टिव रखा जाए. इससे उसे अपना कॉल लेटर/साक्षात्कार संबंधी सूचना आदि ईमेल के माध्यम से प्राप्त करने में सहायता होगी.

ऑनलाइन आवेदन करने के लिए दिशानिर्देश:

i. उम्मीदवार एसबीआई की वेबसाइट **https://sbi.bank.in/web/careers/current-openings** पर उपलब्ध लिंक के माध्यम से अपना ऑनलाइन पंजीकरण करें और इन्टरनेट बैंकिंग/ डेबिट कार्ड/ क्रेडिट कार्ड/ यूपीआई आदि का उपयोग करके आवेदन शुल्क का भुगतान करें.

ii. उम्मीदवार सर्वप्रथम अपने नवीनतम फोटो और हस्ताक्षर स्कैन करें. ऑनलाइन आवेदन तब तक पंजीकृत नहीं होगा जब तक कि उम्मीदवार अपनी फोटो और हस्ताक्षर ऑनलाइन पंजीकरण पेज पर बताए अनुसार अपलोड ('दस्तावेज अपलोड कैसे करें' के अंतर्गत) नहीं कर देता/देती.

iii. उम्मीदवार आवेदन को ध्यानपूर्वक भरें. आवेदन पूरी तरह से भरने के बाद ही इसे प्रस्तुत करें. यदि एक बार में उम्मीदवार आवेदन नहीं भर पाता है, तो वह पहले से प्रविष्ट जानकारी को सेव कर सकता/सकती है. जब जानकारी/आवेदन को सेव किया जाएगा तो एक अनंतिम पंजीकरण नंबर और पासवर्ड सिस्टम द्वारा जनरेट किया जाएगा और यह स्क्रीन पर प्रदर्शित होगा. **उम्मीदवार इस पंजीकरण नंबर और पासवर्ड को नोट कर लें.** वे इस सेव किए हुए आवेदन को पंजीकरण नंबर और पासवर्ड का प्रयोग कर फिर से खोल सकते हैं और यदि आवश्यक हो तो दिए गए विवरण में संशोधन कर सकते हैं. सेव की गई जानकारी को इस तरह से बदल कर संशोधन करने की अनुमति मात्र तीन बार तक होगी. आवेदन के पूरी तरह भर जाने उम्मीदवार इसे प्रस्तुत करें और ऑनलाइन शुल्क का भुगतान करें.

iv. **ऑनलाइन पंजीकरण के बाद, उम्मीदवारों को यह सूचना दी जाती है कि वे सिस्टम के बनाए ऑनलाइन आवेदन प्रपत्रों को प्रिन्ट कर लें.**

v. आयु सीमा में छूट चाहने वाले उम्मीदवारों को दस्तावेज़ सत्यापन करते समय जरूरी प्रमाणपत्र (पत्रों) की प्रतियां प्रस्तुत करनी होगी. ऑनलाइन आवेदन पंजीकरण के पश्चात, किसी उम्मीदवार की श्रेणी में कोई परिवर्तन संभव नहीं है.

शुल्क भुगतान के लिए दिशानिर्देश:

i. सामान्य/ओबीसी/ईडब्ल्यूएस उम्मीदवारों के लिए आवेदन शुल्क और सूचना प्रभार (वापस न करने योग्य) ₹750/- है (सात सौ पचास रुपए मात्र) और अनुसूचित जाति/अनुसूचित जनजाति/बेंचमार्क दिव्यांग व्यक्ति के उम्मीदवारों के लिए कोई शुल्क/सूचना प्रभार नहीं है.

ii. आवेदन पत्र के विवरण सही हैं यह सुनिश्चित कर लेने के बाद उम्मीदवार द्वारा आवेदन के साथ एकीकृत भुगतान गेटवे के माध्यम से शुल्क का भुगतान करना होगा. इसके बाद आवेदन में कोई परिवर्तन/संशोधन की अनुमति नहीं दी जाएगी.

iii. शुल्क का भुगतान वहां उपलब्ध भुगतान गेटवे के माध्यम से ऑनलाइन ही करना होगा. भुगतान डेबिट कार्ड/क्रेडिट कार्ड/इन्टरनेट बैंकिंग/यूपीआई आदि द्वारा स्क्रीन पर बताई जानकारी के अनुसार किया जा सकता है. ऑनलाइन भुगतान करते समय यदि कोई लेनदेन शुल्क लागू हो तो वह उम्मीदवारों को ही वहन करना होगा.

iv. भुगतान कार्य सफलतापूर्वक हो जाने के बाद उम्मीदवार द्वारा प्रस्तुत किए जाने की तारीख के साथ ई-रसीद और आवेदन फॉर्म बनेगा जिसे प्रिन्ट कर उम्मीदवार अपने पास रख लें.

v. यदि पहली बार में ऑनलाइन शुल्क का भुगतान नहीं हो पाता है, तो ऑनलाइन भुगतान के लिए फिर से प्रयास करें.

vi. शुल्क विवरणों सहित ई-रसीद और आवेदन फॉर्म का प्रिन्ट फिर से करने का भी प्रावधान है.

vii. **एक बार भुगतान किया गया आवेदन शुल्क किसी भी कारण से वापस नहीं लौटाया जाएगा, न ही इसे किसी अन्य परीक्षा या भावी चयन के लिए समायोजित किया जाएगा.**

ज. दस्तावेज़ अपलोड कैसे करें:

अ. अपलोड किए जाने वाले दस्तावेज़ का विवरण:

i. नवीनतम फोटोग्राफ
ii. हस्ताक्षर
iii. बायोडाटा (प्रारूप संलग्न) (पीडीएफ)
iv. जीवन वृत्त (पीडीएफ)
v. आईडी प्रमाण (पीडीएफ)
vi. जन्म तिथि का प्रमाण (पीडीएफ)
vii. शैक्षणिक योग्यता: संबंधित अंक तालिका/डिग्री प्रमाणपत्र (पीडीएफ)
viii. अनुभव प्रमाणपत्र (पीडीएफ)
ix. जाति प्रमाणपत्र/ईडब्ल्यूएस प्रमाणपत्र, (यदि लागू हो) (पीडीएफ)
x. पीडब्ल्यूबीडी प्रमाणपत्र, (यदि लागू हो) (पीडीएफ)
xi. अधिमान्य योग्यता/प्रमाणपत्र (यदि कोई हो) (पीडीएफ)
xii. फॉर्म-16/ऑफर लेटर/वर्तमान नियोक्ता से नवीनतम वेतन पर्ची (पीडीएफ)

ब. फोटोग्राफ फाइल टाइप/साइज़:

i. पासपोर्ट आकार की नवीनतम रंगीन फोटो होनी चाहिए.
ii. फाइल का आकार 20 केबी-50 केबी और डायमेंशन 200X230 पिक्सल (अधिमानत:) तक होना चाहिए.
iii. यह सुनिश्चित कर लें कि फोटो रंगीन है, और सफेद या हल्के रंग की पृष्ठभूमि में लिया गया हो.
iv. तनावमुक्त होकर कैमरे में सामने की ओर देखें.
v. फोटो यदि धूप में ली गई हो तो सूरज आपके पीछे रहे या आप छाया में हों ताकि आपकी नज़र में तिरछापन न आए या फिर कोई छाया न पड़े.
vi. यदि आपको फ्लैश का प्रयोग करना है, तो यह सुनिश्चित करें कि इसमें रेड-आई नहीं है.
vii. यदि आप चश्मा लगाते हैं, तो यह सुनिश्चित करें कि कोई परछाई नहीं पड़ रही है और आपकी आंखें साफ देखी जा सकती हैं.
viii. टोपी, हैट और गहरे रंग का चश्मा लगाया जाना स्वीकार्य नहीं है. धार्मिक प्रतीक पगड़ी आदि बांध सकते हैं लेकिन इससे आपका चेहरा न ढकने पाए.
ix. यह सुनिश्चित करें कि स्कैन किया गया चित्र 50 केबी से अधिक का नहीं है. फाइल का आकार यदि 50 केबी से अधिक का है, तो स्कैनिंग की प्रक्रिया के दौरान डीपीआई रिजोल्यूशन, रंगों की संख्या आदि जैसी बातें स्कैनर पर सेट कर लें.

स. हस्ताक्षर फाइल का प्रकार/आकार:

i. आवेदक सफेद कागज पर काली पेन से हस्ताक्षर करें.
ii. हस्ताक्षर आवेदक स्वयं करें न कि कोई अन्य व्यक्ति.
iii. कॉल लेटर तथा जहां आवश्यक होंगे वहां हस्ताक्षर का उपयोग किया जाएगा.
iv. फाइल का आकार 10 केबी-20 केबी के बीच का हो और डायमेंशन 140X60 पिक्सल (अधिमानत:) हो.
v. यह सुनिश्चित करें कि स्कैन किए गए चित्र का आकार 20 केबी से अधिक नहीं है.
vi. अंग्रेज़ी के केपिटल लेटर में किए गए हस्ताक्षर स्वीकार्य नहीं होंगे.

द. दस्तावेज़ की फाइल का प्रकार/आकार:

i. सभी दस्तावेज़ पीडीएफ प्रारूप में हों. (फोटोग्राफ और हस्ताक्षर को छोड़कर)
ii. दस्तावेज़ के पृष्ठ का आकार ए4 का हो.
iii. फाइल का आकार 500 केबी से अधिक का न हो.
iv. दस्तावेज़ को यदि स्कैन किया जा रहा है तो आप यह सुनिश्चित करें कि इसे पीडीएफ के रूप में सेव कर लिया गया है और इसका आकार पीडीएफ के तौर पर 500 केबी से अधिक का नहीं है. फाइल का आकार यदि 500 केबी से अधिक का है तो स्कैनर की सेटिंग की प्रक्रिया के दौरान डीपीआई का रिज़ोल्यूशन, रंगों की संख्या आदि समायोजित करें. यह सुनिश्चित कर लें कि अपलोड किए गए दस्तावेज़ साफ और पढ़े जा सकने योग्य हैं.

य. फोटो/हस्ताक्षर/दस्तावेज़ को स्कैन करने हेतु दिशा-निर्देश:

i. स्कैनर के रिज़ोल्यूशन को कम से कम 200 डीपीआई (डॉट्स पर इन्च) पर रखें.
ii. कलर को ट्रू कलर पर सेट करें.
iii. फोटो/हस्ताक्षर के किनारे तक क्रॉप करके इमेज को स्कैन करें फिर इमेज को अंतिम आकार (जैसा ऊपर बताया गया है) देने के लिए क्रॉप करने हेतु अपलोड एडिटर का प्रयोग करें.
iv. फोटो/हस्ताक्षर की फाइल जेपीजी या जेपीईजी प्रारूप में हो (यानी फाइल का नाम image01.jpg या image01.jpeg दिखाई दे)
v. इमेज के आयाम फोल्डर/फाइल की लिस्टिंग कर जांचे जा सकते हैं या फिर फाइल इमेज के आइकन पर माउस को घुमाकर इसे जांचा जा सकता है
vi. जो उम्मीदवार एमएस विन्डोज़/एमएस ऑफिस का प्रयोग करते हैं, वे आसानी से फोटो और हस्ताक्षर जेपीईजी फार्मेट में पा सकते हैं जो कि क्रमश: 50 केबी और 20 केबी से अधिक न होगी, इसके लिए एमएस पेन्ट या एमएस ऑफिस पिक्चर मैनेजर का प्रयोग करना होगा. स्कैन किया गया फोटो या हस्ताक्षर किसी भी फार्मेट सें जेपीजी (jpg) फार्मेट में सेव किए जा सकते हैं. इसके लिए फाइल मेन्यू में 'सेव ऐज़' के विकल्प का प्रयोग करना होगा. इमेज मेन्यू द्वारा क्रॉप और रिसाइज़ (बिंदु 1 और 2 ऊपर देखें जो कि पिक्स्ल आकार के लिए दिया हुआ है) विकल्प चुनकर फाइल के आकार को 50 केबी (फोटो) और 20 केबी (हस्ताक्षर) से कम किया जा सकता है. इसी तरह के विकल्प अन्य फोटो एडीटर में भी उपलब्ध हैं.
vii. ऑनलाइन आवेदन फार्म भरते समय उम्मीदवार को एक लिंक उपलब्ध करवाया जाएगा ताकि वह अपने फोटो और हस्ताक्षर को अपलोड कर सके.

र. दस्तावेज़ अपलोड करने की प्रक्रिया:

i. प्रत्येक दस्तावेज़ को अपलोड करने हेतु अलग-अलग लिंक दिए गए है.
ii. ''अपलोड'' का संबंधित लिंक क्लिक करें.
iii. ब्राउज़ करके उस जगह को चुनें जहां कि जेपीजी या जेपीईजी, पीडीएफ, डीओसी या डीओसीएक्स फाइल को सेव किया गया है.
iv. फाइल पर क्लिक कर इसे चुनें और अपलोड का बटन क्लिक करें.
v. आवेदन सबमिट करने से पहले प्रलेख अपलोड हो गया है और सही तरह से खुल रहा है, इस बात की पुष्टि करने के लिए प्रिव्यू क्लिक करें. यदि फाइल का आकार और प्रारूप बताए अनुसार नहीं है तो इसमें त्रुटि का संदेश आएगा.
vi. दस्तावेज़ अपलोड हो जाने के बाद/प्रस्तुत कर दिए जाने के बाद संशोधित/परिवर्तित नहीं हो सकेंगे.
vii. **ऑनलाइन आवेदन फार्म में फोटो/हस्ताक्षर अपलोड कर दिए जाने के बाद उम्मीदवार जांच लें कि फोटो साफ हैं और ये ठीक तरह से अपलोड हुए हैं.** फोटो या हस्ताक्षर स्पष्ट रूप से यदि नहीं दिखें तो उम्मीदवार अपने आवेदन को संशोधित कर सकता/सकती है और अपने फोटो या हस्ताक्षर आवेदन फार्म प्रस्तुत किए जाने से पहले फिर से अपलोड कर सकता/सकती है. **फोटो पर चेहरा या हस्ताक्षर यदि स्पष्ट नहीं हैं तो उम्मीदवार का आवेदन अस्वीकार किया जा सकता है.**

झ. सामान्य जानकारी:

i. पद के लिए आवेदन करने से पहले आवेदक को यह सुनिश्चित करना चाहिए कि वह पद के लिए उपर्युक्त वर्णित योग्यता और अन्य मानदंडों को निर्दिष्ट तारीख को पूरा करता/करती है और उसके द्वारा प्रस्तुत विवरण सभी प्रकार से सही है.

ii. आरक्षित श्रेणी के उम्मीदवार, उन उम्मीदवारों को शामिल करके जिनके लिए किसी आरक्षण का वर्णन नहीं किया गया है, सामान्य श्रेणी के लिए घोषित रिक्त पदों के लिए आवेदन करने के लिए स्वतंत्र हैं बशर्ते वे सामान्य श्रेणी के लिए लागू पात्रता की सभी शर्तें पूरी करते हों.

iii. भर्ती के किसी भी स्तर पर यदि ऐसा पता चलता है कि कोई उम्मीदवार पात्रता मानदंडों को पूरा नहीं करता/करती है, तो और/या यह कि उसने गलत/झूठी जानकारी दी है या उसने कोई महत्वपूर्ण जानकारी (जानकारियां) छिपाई हैं तो उसकी उम्मीदवारी को निरस्त कर दिया जाएगा. इनमें से यदि कोई बात उसके नियुक्ति/अंतिम चयन के बाद भी पता चलती है, तो उसकी सेवाएं तुरंत समाप्त की जा सकती हैं.

iv. आवेदक को सुनिश्चित करना चाहिए कि आवेदन पूरी तरह से निर्धारित प्रारूप के अनुसार है और सही एवं पूरी तरह से भरा गया है.

v. चयनित उम्मीदवार कि नियुक्ति बैंक की आवश्यकता के अनुसार चिकित्सकीय रूप से उपयुक्त घोषित किए जाने के अधीन है. इस तरह कि नियुक्ति बैंक में ऐसे पद के लिए बैंक के सेवा और आचरण नियमों के अधीन भी होगी, जो बैंक में भर्ती होने के समय लागू है.

vi. उम्मीदवारों को सूचित किया जाता है कि वे संप्रेषण जैसे कॉल लेटर/साक्षात्कार की तारीख की सूचना, आदि प्राप्त करने के लिए अपने ई–मेल आईडी एवं मोबाईल फोन नंबर को एक्टिव रखें.

vii. किसी संप्रेषण की प्राप्ति में विलंब होने या न मिलने के लिए बैंक की कोई जिम्मेदारी नहीं होगी.

viii. जो उम्मीदवार सरकार/अर्ध–सरकारी कार्यालयों, बैंकों और वित्तीय संस्थानों सहित सार्वजनिक क्षेत्र के प्रतिष्ठानों में कार्यरत हैं, उन्हें सूचित करते हैं कि वे साक्षात्कार के समय अपने नियोक्ता से अनापत्ति प्रमाणपत्र लेकर प्रस्तुत करें, ऐसा न करने पर उनकी उम्मीदवारी पर विचार नहीं किया जाएगा और वे यदि किसी यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे, तो उन्हें उसका भुगतान नहीं किया जाएगा.

ix. चयन होने पर, उम्मीदवार से अपेक्षा होगी कि वह नियुक्ति प्राप्त करते समय अपने नियोक्ता का उचित डिस्चार्ज सर्टिफिकेट प्रस्तुत करें.

x. उम्मीदवारों को उनके हित के लिए यह सूचना दी जाती है कि वे अंतिम तारीख से पहले समय रहते ही ऑनलाइन आवेदन प्रस्तुत कर दें और वे अंतिम तारीख का इंतज़ार न करते रहें क्योंकि बाद में हो सकता है कि वेबसाइट में लॉग ऑन करने में डिसकनेक्शन/अक्षमता/फेलियर की स्थिति बन जाए इन्टरनेट पर भारी लोड या फिर वेबसाइट जाम होने के कारण ऐसा हो जाए. पूर्वोक्त कारणों से एसबीआई के नियंत्रण से बाहर के किसी भी कारण से यदि उम्मीदवार अपना आवेदन समय रहते नहीं कर पाते हैं, तो इसके लिए एसबीआई किसी भी तरह से जिम्मेदार नहीं होगा.

xi. पात्रता, साक्षात्कार आयोजित किए जाने, अन्य परीक्षाएं और चयन के सभी मामलों में बैंक के निर्णय अंतिम और सभी उम्मीदवारों के लिए बाध्यकारी होंगे. इस संबंध में किसी अभ्यावेदन पर विचार नहीं किया जाएगा और न ही इस संबंध में कोई पत्र–व्यवहार किया जाएगा.

xii. आवेदन में दी गई जानकारी बाद में गलत पाए जाने पर आवेदक पर दीवानी/फौजदारी मुकदमा किया जा सकता है.

xiii. पात्रता संबंधी मानदंड पूरा करने मात्र से उम्मीदवार साक्षात्कार के लिए बुलाए जाने का हकदार नहीं है. बैंक के पास उम्मीदवार की योग्यता, उपयुक्तता, अनुभव आदि के संबंध में प्रारंभिक जांच/शॉर्टलिस्टिंग करने के बाद उचित संख्या में ही उम्मीदवारों को साक्षात्कार के लिए बुलाए जाने का अधिकार सुरक्षित है.

xiv. एक से अधिक आवेदन के मामले में, केवल अंतिम वैध (पूर्ण) आवेदन को बरकरार रखा जाएगा और अन्य पंजीकरण के लिए भुगतान किया गया आवेदन शुल्क/सूचना शुल्क जब्त कर लिया जाएगा.

xv. इस विज्ञापन और/या इसके जवाब में आए आवेदन के कारण किसी दावे या विवाद की दशा में कानूनी कार्यवाही केवल मुंबई और मुंबई स्थित न्यायालयों/न्यायाधिकरणों/मंचों पर ही की जा सकती हैं. किसी भी मुकदमे/विवाद की सुनवाई का एकल व एकमात्र अधिकार क्षेत्र मुंबई ही होगा.

xvi. शॉर्टलिस्टिंग के बाद साक्षात्कार के लिए बुलाये जाने वाले बाहरी उम्मीदवारों को उनके निवास स्थान या वर्तमान पोस्टिंग के स्थान से भारत में सबसे छोटे मार्ग के लिए हवाई टिकट (इकोनॉमी क्लास) का यात्रा किराया 10,000/- रुपये (दोनों तरफ के लिए कुल) तक या वास्तविक खर्च (जो भी कम हो) की प्रतिपूर्ति की जाएगी जो वास्तविक यात्रा के आधार पर टिकटों की प्रतियां प्रस्तुत करने के अधीन है. स्थानीय वाहन जैसे टैक्सी/कैब/निजी वाहन व्यय/किराया देय/प्रतिपूर्ति योग्य नहीं होगा. यदि कोई उम्मीदवार को पद के लिए अपात्र पाया जाता है, तो उसे साक्षात्कार के लिए उपस्थित होने की अनुमति नहीं दी जाएगी और किसी भी किराए की प्रतिपूर्ति नहीं की जाएगी.

xvii. आवेदन पत्र एक बार प्रस्तुत कर दिए जाने पर उसमें किसी भी विवरण (श्रेणी सहित) में परिवर्तन/ सुधार के लिए अनुरोध पर किसी भी परिस्थिति में विचार नहीं किया जाएगा. इस संबंध में किसी पत्राचार/फोन/ईमेल पर विचार नहीं किया जाएगा. उम्मीदवारों को सूचना दी जाती है कि वे ऑनलाइन आवेदन को सावधानी से भरें और आवेदन में सही जानकारी प्रस्तुत करें.

xviii. **बैंक किसी भी विशेष पद/सभी पदों के लिए किसी भी स्तर/समय पर बिना कोई कारण बताए भर्ती प्रक्रिया को पूरी तरह या आंशिक रूप से रद्द/संशोधित करने का अधिकार सुरक्षित रखता है.**

xix. **साक्षात्कार के समय, उम्मीदवार को उसके विरुद्ध लंबित आपराधिक मामलों (यदि कोई हों) का विवरण देना आवश्यक होगा.**

महत्वपूर्ण तथ्यों को छिपाने पर किसी भी समय उम्मीदवारी रद्द/समाप्त कर दी जाएगी, भले ही उम्मीदवार का चयन हो गया हो, ऐसी परिस्थितियों में उसका चयन रद्द कर दिया जाएगा. बैंक अन्य बातों के साथ–साथ पुलिस रिकॉर्ड के सत्यापन सहित स्वतंत्र सत्यापन भी कर सकता है. बैंक ऐसे प्रकटनों और/या सत्यापन के आधार पर नियुक्ति से इनकार करने का अधिकार अपने पास सुरक्षित रखता है.

किसी जानकारी के लिए, कृपया बैंक की वेबसाइट (https://sbi.bank.in/web/careers/post-your-query) पर उपलब्ध "CONTACT US/post your query" लिंक के माध्यम से हमसे संपर्क करें.

मुद्रण की त्रुटियाँ यदि हों, तो उसके लिए बैंक उत्तरदायी नहीं होगा.
किसी विवाद की स्थिति में अंग्रेजी में जारी विज्ञापन मान्य होगा.

भारतीय स्टेट बैंक किसी भी ऐसे बाहरी कोचिंग प्लेटफॉर्म, कंसल्टेंसी, व्यक्ति या डिजिटल चैनल का समर्थन, विज्ञापन या उनके साथ जुड़ाव नहीं रखता है, जो चयन की गारंटी, भर्ती प्रक्रिया को प्रभावित करने या आंतरिक मार्गदर्शन प्रदान करने का दावा करते हैं. उम्मीदवारों को केवल एसबीआई के आधिकारिक करियर पोर्टल पर उपलब्ध जानकारी पर ही भरोसा करना चाहिए.

मुंबई
24.02.2026

महाप्रबंधक
(आरपी एवं पीएम)

आवेदन कैसे करें

https://sbi.bank.in/web/careers/current-openings पर लॉगिन करें

नीचे स्क्रॉल करें और संबंधित विज्ञापन पर क्लिक करें

विज्ञापन सं. CRPD/SCO/2025-26/25 डाउनलोड करें
(विस्तृत विज्ञापन ध्यानपूर्वक पढ़ें)

ऑनलाइन आवेदन करें
(अंतिम प्रस्तुतीकरण से पहले, कृपया अपना आवेदन अच्छी तरह पढ़ लें. अंतिम प्रस्तुतीकरण के बाद उसमें सुधार की अनुमति नहीं दी जाएगी)