# भारतीय स्टेट बैंक

केंद्रीय भर्ती एवं पदोन्नति विभाग, कॉर्पोरेट केंद्र, मुंबई

फोन: 022-2282 0427, ईमेल: crpd@sbi.co.in


## एसबीआई ने इकोनॉमिक्स टाइम्स ह्यूमन कैपिटल अवार्ड्स 2026 में 4 श्रेणियों में स्वर्ण पदक जीतकर शानदार प्रदर्शन किया.

# संविदा/नियमित आधार पर विशेषज्ञ संवर्ग के अधिकारियों की भर्ती

## (विज्ञापन सं.: CRPD/SCO/2026-27/11)

## आवेदन का ऑनलाइन पंजीकरण और शुल्क का भुगतान: दिनांक 07.08.2026 से 27.08.2026 तक

**भारतीय स्टेट बैंक संविदा/नियमित आधार पर विशेषज्ञ संवर्ग के निम्नलिखित पदों 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.**

**भर्ती का संक्षिप्त सारांश: पद: कई पद (कट-ऑफ तारीख: 31.07.2026)**

| पद | आयु (वर्षों में) | शैक्षणिक योग्यता | अनुभव |
|---|---|---|---|
| **डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब** | **न्यूनतम – 35 वर्ष<br>अधिकतम – 45 वर्ष** | **योग्यता:** भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री.<br>**या**<br>भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एम.ई./ एमटेक/ एमएसई. | कुल 12+ वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष का अनुभव प्रौद्योगिकी नवोन्मेषण/ आईटी नवोन्मेषण/ डिजिटल नवोन्मेषण/ उभरती प्रौद्योगिकी/ साइबर सुरक्षा नवोन्मेषण/ प्रौद्योगिकी रणनीति/ इनोवेशन लैब्स/ सेंटर ऑफ एक्सीलेंस (CoE), डिजिटल ट्रांसफॉर्मेशन/ उत्पाद नवोन्मेषण/ प्रौद्योगिकी परामर्श या संबंधित क्षेत्रों में हो. |
| **डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक-केंद्रित पहल** | | | बीएफएसआई आईटी/ सूचना सुरक्षा/ साइबर सुरक्षा में न्यूनतम 12 वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष साइबर सुरक्षा/ साइबर सुरक्षा जागरूकता कार्यक्रम चलाने का अनुभव हो. |
| **उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा** | | | बीएफएसआई आईटी/ सूचना सुरक्षा/ साइबर सुरक्षा में न्यूनतम 12 वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष साइबर अनुसंधान/ साइबर डिफेंस और इंटेलिजेंस का अनुभव हो. |
| **उप प्रबंधक – एआई विशेषज्ञ** | **न्यूनतम – 25 वर्ष<br>अधिकतम – 35 वर्ष** | कंप्यूटर साइंस/ कंप्यूटर साइंस एवं इंजीनियरिंग/डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/ सॉफ्टवेयर इंजीनियरिंग/ सूचना प्रौद्योगिकी/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या ऊपर निर्दिष्ट विषयों में कम से कम 50% अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>कंप्यूटर साइंस/ कंप्यूटर साइंस एवं इंजीनियरिंग/ सूचना प्रौद्योगिकी/ डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में समतुल्य डिग्री. | सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव. इन 4 वर्षों में से, 2 वर्ष का अनुभव इन कामों में होना चाहिए: एमएल/ डीप लर्निंग मॉडल डिज़ाइन करना/ वर्कफ़्लो मैपिंग/ GenAI/ आरएजी पाइपलाइन डिप्लॉय करना/ सुरक्षित एपीआई डिप्लॉयमेंट/ एडब्ल्यूएस सेजमेकर, गूगल क्लाउड वर्टेक्स एआई या माइक्रोसाफ्ट एज्योर एमएल जैसे क्लाउड एमएल सूट का अनुभव/ टेन्सरफ्लो, पाइटॉर्च, साइकिट-लर्न, पैंडास, एक्सजीबूस्ट, हगिंग फेस, लैंग चेन, ओपन एआई एपीआई, अपाचे स्पार्क, पाइथन, प्रॉम्प्ट इंजीनियरिंग, फाइन ट्यूनिंग जैसी लाइब्रेरीज़ में महारत. |
| **उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ** | **न्यूनतम – 25 वर्ष<br>अधिकतम – 35 वर्ष** | कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सॉफ्टवेयर इंजीनियरिंग/ इंफॉर्मेशन टेक्नोलॉजी/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में बी.टेक/ बी.ई. या ऊपर निर्दिष्ट विषयों में कम से कम 50% अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सूचना प्रौद्योगिकी/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में इसके समतुल्य डिग्री. | न्यूनतम अनुभव: साइबर सुरक्षा/ सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव. |
| **उप प्रबंधक – साइबर सुरक्षा एनालिस्ट** | **न्यूनतम – 25 वर्ष<br>अधिकतम – 35 वर्ष** | कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सॉफ्टवेयर इंजीनियरिंग/ इंफॉर्मेशन टेक्नोलॉजी/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में बी.टेक/ बी.ई. या ऊपर निर्दिष्ट विषयों में कम से कम 50% अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सूचना प्रौद्योगिकी/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में इसके समतुल्य डिग्री. | न्यूनतम अनुभव: साइबर सुरक्षा/ सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव. |

## महत्वपूर्ण सूचनाएँ:

1. उम्मीदवारों से अनुरोध है कि वे आवेदन करने से पहले, यह सुनिश्चित करें कि वे पात्रता तिथि तक उक्त पद के लिए दिए गए योग्यता मानदंडों को पूरा करते हों. उम्मीदवारों को वेबसाइट **https://sbi.bank.in/web/careers/current-openings** के माध्यम सें 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 इन पदों के लिए 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 पर ऑनलाइन आवेदन प्रस्तुत कर दें और वे अंतिम तारीख का इंतज़ार न करें. 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, उम्मीदवार यह जांच लें कि उन्होंने आवेदन पत्र के प्रत्येक संबंधित क्षेत्र में सही विवरण भरा है. ऑनलाइन आवेदन की समय-सीमा 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 के पास 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/नियुक्त किए गए अधिकारियों को भारत में स्थित भारतीय स्टेट बैंक के किसी भी कार्यालय में तैनात/स्थानांतरण 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. **किसी भी परिवर्तन/अद्यतन की अलग से सूचना नहीं दी जाएगी. 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 दस्तावेज़ सत्यापन के समय मांगे जाने पर निर्धारित प्रारूप में सक्षम प्राधिकारी का वैध अपेक्षित प्रमाण पत्र प्रस्तुत करना होगा. 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 इस पद के लिए आवेदन करने के लिए पात्र नहीं हैं. यदि शॉर्टलिस्ट किए गए/चयनित उम्मीदवारों के विरुद्ध ऐसी 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 पाए जाने पर उसकी उम्मीदवारी को सरासरी तौर पर अस्वीकृत/रद्द कर दिया जाएगा.

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/छद्मरुपण 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 वर्तमान भर्ती नीति के अनुसार परिवीक्षा पर रहेंगे.

19. इस परियोजना के अतंर्गत 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 वे 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 सरकारी/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 यदि वे किसी यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे, तो उन्हें उसका भुगतान नहीं किया जाएगा.

25. आर्थिक रूप से कमजोर वर्ग (EWS) की श्रेणी में आवेदन करने वाले उम्मीदवारों को **वित्तीय वर्ष 2025-26 की आय के आधार पर ईडब्ल्यूएस प्रमाणपत्र** जमा करना होगा. ऐसा न करने पर उनकी उम्मीदवारी पर विचार नहीं किया जाएगा और अगर कोई यात्रा खर्च मिलने वाला होता, तो वह भी नहीं दिया जाएगा.

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

**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^ (31.07.2026 तक) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | अनारक्षित | अ.जा. | अ.ज.जा. | अ.पि.व. | ईडब्ल्यूएस | कुल | वीआई | न्यूनतम | अधिकतम |
| **1.** | **डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब** | **संविदात्मक (एमएमजीएस-V)** | 1 | -- | -- | -- | -- | 1 | -- | 35 | 45 |
| **2.** | **डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक-केंद्रित पहल** | | 1 | -- | -- | -- | -- | 1 | -- | | |
| **3.** | **उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा** | | 2 | -- | -- | -- | -- | 2 | 1 | | |
| **4.** | **उप प्रबंधक – एआई विशेषज्ञ** | **नियमित** | 12 | 4 | **1** | 6 | 2 | 25 | 1 | 25 | 35 |
| **5.** | **उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ** | | 2 | -- | -- | -- | -- | 2 | 1 | | |
| **6.** | **उप प्रबंधक – साइबर सुरक्षा एनालिस्ट** | | 2 | -- | -- | 1 | -- | 3 | 1 (बैकलॉग) | | |
| **कुल** | | | **22** | **4** | **1** | **7** | **2** | **34** | **4** | | |

**#** - समस्तरीय रिक्तियाँ.

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

**संक्षेपाक्षर: अना –** अनारक्षित; **अ.पि.व.** – अन्य पिछड़ा वर्ग; **अ.जा.** – अनुसूचित जाति, **अ.ज.जा.** – अनुसूचित जनजाति; **ईडब्ल्यूएस** – आर्थिक रूप से कमजोर वर्ग; **पीडब्ल्यूबीडी –** निर्धारित बेंचमार्क दिव्यांगता वाले व्यक्ति; **वीआई –** दृष्टि बाधित;

**महत्वपूर्ण बिंदु:**

1. पीडब्ल्यूबीडी उम्मीदवारों के लिए आरक्षण समस्तरीय है और संबंधित मूल श्रेणी की समग्र रिक्ति में शामिल है (जहां लागू हो).
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 के दिशानिर्देशों के अनुसार होगा (जहां लागू हो).
6. ऐसे उम्मीदवार जो ओबीसी श्रेणी से संबंधित हैं लेकिन 'क्रीमी लेयर' में 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 चाहने वाले उम्मीदवारों द्वारा निर्धारित प्रारूप में एक घोषणा जमा करवानी होगी कि वह आवेदन के ऑनलाइन पंजीकरण की अंतिम तिथि को क्रीमी लेयर के अंतर्गत नहीं है. **यदि उन्हें साक्षात्कार के लिए बुलाया जाता है, तो ऐसे उम्मीदवारों को 01.04.2026 से साक्षात्कार की तिथि के दौरान जारी किया गया 'नॉन क्रीमी लेयर' से संबंधित ओबीसी प्रमाण-पत्र, जमा करना होगा.** 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. आर्थिक रूप से कमजोर वर्ग (EWS) के उम्मीदवारों को साक्षात्कार के समय दस्तावेज सत्यापन की तारीख पर, **कार्मिक एवं प्रशिक्षण विभाग के मौजूदा नियमों के अनुसार, वित्तीय वर्ष 2025-26 की कुल वार्षिक आय के आधार पर जारी और वर्ष 2026-27 के लिए मान्य 'आय एवं संपत्ति प्रमाणपत्र'** सत्यापन के लिए दिखाना होगा. वित्तीय वर्ष 2025-26 की कुल वार्षिक आय के आधार पर जारी 'आय एवं संपत्ति प्रमाणपत्र' उम्मीदवारों को साक्षात्कार के समय दस्तावेज सत्यापन की तारीख या उससे पहले हासिल कर लेना चाहिए. **निर्धारित तारीख के बाद 'आय एवं संपत्ति प्रमाणपत्र' दिखाने के लिए समय बढ़ाने की किसी भी अनुरोध पर विचार नहीं किया जाएगा** और अगर कोई उम्मीदवार साक्षात्कार के समय 'आय एवं संपत्ति प्रमाणपत्र' नहीं दिखा पाता है, तो उसे साक्षात्कार में शामिल होने की अनुमति नहीं दी जाएगी और बैंक में उस पद पर नियुक्ति के लिए उस पर विचार नहीं किया जाएगा.
9. निर्धारित बेंचमार्क दिव्यांग व्यक्ति (पीडब्ल्यूबीडी), सहित आरक्षित श्रेणी से संबंधित सभी उम्मीदवार जिनके लिए आरक्षण का कोई उल्लेख नहीं किया गया है, 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.
10. 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 प्राप्त किया जा सकता है.
11. 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.

12. पीडब्ल्यूबीडी उम्मीदवार को भारत सरकार के दिशानिर्देशों के अनुसार सक्षम प्राधिकारी द्वारा जारी प्रमाणपत्र प्रस्तुत करना होगा (जहां लागू हो).
13. 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 है और जहाँ विनिर्दिष्ट दिव्यांगता को मापन श्रेणी में नहीं रखा गया है. लेकिन 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 में 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 रद्द/अस्वीकृत की जा सकती है 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 - डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:** योग्यता: भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री.<br>**या**<br>भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एम.ई./ एमटेक/ एमएसई. |
| **अन्य योग्यता (31.07.2026 तक)** | **अधिमान्य प्रमाणन:** CISSP, CISM, CISA, CCSP, PMP, MBA (प्रौद्योगिकी प्रबंधन)<br>**(प्रमाणन रजिस्ट्रेशन की अंतिम तारीख तक मान्य होना चाहिए.)** |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:**<br>कुल 12+ वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष का अनुभव प्रौद्योगिकी नवोन्मेषण/ आईटी नवोन्मेषण/ डिजिटल नवोन्मेषण/ उभरती प्रौद्योगिकी/ साइबर सुरक्षा नवोन्मेषण/ प्रौद्योगिकी रणनीति/ इनोवेशन लैब्स/ सेंटर ऑफ एक्सीलेंस (CoE), डिजिटल ट्रांसफॉर्मेशन/ उत्पाद नवोन्मेषण/ प्रौद्योगिकी परामर्श या संबंधित क्षेत्रों में हो.<br>**प्राथमिकता:**<br>• साइबर–सुरक्षा नवोन्मेषण पहल और साइबर समाधानों के सिमुलेशन पर काम करने या उनका प्रबंध करने का अनुभव.<br>• आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर–सुरक्षा सेटअप, परामर्शी संगठनों या संबंधित क्षेत्रों में साइबर– सुरक्षा भूमिकाओं का अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवोन्मेषण, साइबर डिफेंस या संबंधित क्षेत्रों में काम किया हो.<br>• सेंटर ऑफ एक्सीलेंस (CoE) स्थापित करने या उसमें काम करने का अनुभव.<br>**शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • मज़बूत नेतृत्व और प्रबंध कौशल, साथ ही टीम को प्रेरित और प्रोत्साहित करने की क्षमता.<br>• साइबर–सुरक्षा डोमेन की अच्छी तकनीकी जानकारी.<br>• तकनीकी कौशल के प्रशिक्षण और प्रसार, ज़रूरतों की पहचान करना और स्किलिंग व जागरूकता कार्यक्रमों की ज़िम्मेदारी लेना.<br>• साइबर लैब्स और आधुनिक लर्निंग टेक्नोलॉजी की जानकारी.<br>• उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल, साथ ही अलग–अलग तरह के लोगों को जटिल तकनीकी संकल्पनाओं समझाने की क्षमता.<br>• मज़बूत परियोजना प्रबंध कौशल, जिसमें जटिल प्रशिक्षण कार्यकम की योजना बनाने, उन्हें व्यवस्थित करने और लागू करने की क्षमता हो.<br>• साइबर सुरक्षा प्रशिक्षण और शिक्षा से जुड़ी जटिल समस्याओं की पहचान करने और उन्हें हल करने की क्षमता। बदलती टेक्नोलॉजी और उद्योग की प्रवृत्तियों के अनुसार स्वयं को ढालने की क्षमता.<br>• पब्लिक–प्राइवेट पार्टनरशिप मॉडल या सेंटर ऑफ़ एक्सीलेंस का अनुभव.<br>• बीएफएसआई क्षेत्र में साइबर सुरक्षा और उससे जुड़े जोखिमों की गहरी समझ. |

| पद संख्या/पद नाम | 2 - डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक–केंद्रित पहल |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:** मूल योग्यता: भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री.<br>**या**<br>भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एम.ई./ एमटेक/ एमएसई.<br>**प्राथमिकता:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में एडवांस्ड डिग्री. |
| **अन्य योग्यता (31.07.2026 तक)** | **अधिमान्य प्रमाणन:** CISSP, CISM, CISA, CCSP, PMP, MBA (प्रौद्योगिकी प्रबंधन)<br>**(प्रमाणन रजिस्ट्रेशन की अंतिम तारीख तक मान्य होना चाहिए.)** |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:** बीएफएसआई आईटी/ सूचना सुरक्षा/ साइबर सुरक्षा में न्यूनतम 12 वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष साइबर सुरक्षा / साइबर सुरक्षा जागरूकता कार्यक्रम चलाने का अनुभव हो.<br>**प्राथमिकता:**<br>• साइबर सुरक्षा से जुड़ी नागरिकों की जागरूकता गतिविधियों (जैसे अलग–अलग माध्यमों से बड़े पैमाने पर या खास ग्रुप के लिए साइबर जागरूकता कार्यक्रम) में काम करने या उनका प्रबंध करने का अनुभव.<br>• आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर–सुरक्षा सेटअप, परामर्शी संगठनों या संबंधित क्षेत्रों में साइबर– सुरक्षा भूमिकाओं का अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवोन्मेषण, साइबर डिफेंस या संबंधित क्षेत्रों में काम किया हो.<br>• सेंटर ऑफ एक्सीलेंस (CoE) स्थापित करने या उसमें काम करने का अनुभव.<br>**शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • मज़बूत नेतृत्व और प्रबंधन कौशल.<br>• नागरिकों और अंतिम प्रयोक्ता सुरक्षा प्रोग्राम को चलाना, उनकी ज़िम्मेदारी लेना और उनकी प्रभावशीलता को मापना.<br>• आउटरीच और साइबर यूज़र सुरक्षा के लिए प्रोग्राम के विकास को ट्रैक करने के लिए मेट्रिक्स बनाना.<br>• उत्कृष्ट संप्रेषण और अंतर–व्यक्तिगत कौशल.<br>• आईटी, साइबर सुरक्षा और डेटा प्रबंधन जैसे संबंधित क्षेत्रों में तकनीकी विशेषज्ञता.<br>• परियोजना प्रबंधन और प्रोग्राम डिलीवरी का अनुभव.<br>• संबंधित नीतियों, विनियमों और सर्वोत्तम प्रथाओं की जानकारी.<br>• तेज़ी से काम करने वाले माहौल में प्रभावी ढंग से काम करने की क्षमता.<br>• हितधारक जुड़ाव और संबंध प्रबंधन का अनुभव.<br>• नागरिकों पर केंद्रित पहलों में शामिल प्रोफेशनल्स की टीम को मार्गदर्शन देना. |

| **पद संख्या/पद नाम** | **3 - उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा** |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:** मूल योग्यता: भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री.<br>**या**<br>भारत सरकार द्वारा मान्यता प्राप्त या सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एम.ई./ एमटेक/ एमएसई.<br>**प्राथमिकता:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में एडवांस्ड डिग्री. |
| **अन्य योग्यता (31.07.2026 तक)** | **अधिमान्य प्रमाणन:** CISSP, CISM, CISA, CCSP, PMP, MBA (प्रौद्योगिकी प्रबंधन)<br>**(प्रमाणन रजिस्ट्रेशन की अंतिम तारीख तक मान्य होना चाहिए.)** |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:** बीएफएसआई आईटी/ सूचना सुरक्षा/ साइबर सुरक्षा में न्यूनतम 12 वर्ष का अनुभव, जिसमें से कम से कम 6 वर्ष साइबर अनुसंधान / साइबर डिफेंस और इंटेलिजेंस का अनुभव हो.<br>**प्राथमिकता:**<br>• आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर–सुरक्षा सेटअप, परामर्शी संगठनों या संबंधित क्षेत्रों में साइबर– सुरक्षा भूमिकाओं का अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवोन्मेषण, साइबर डिफेंस, साइबर अनुसंधान या संबंधित क्षेत्रों में काम किया हो.<br>• सेंटर ऑफ एक्सीलेंस (CoE) स्थापित करने या उसमें काम करने का अनुभव.<br>**शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • साइबर सुरक्षा के सिद्धांतों, टेक्नोलॉजी और सर्वोत्तम प्रथाओं की गहरी समझ.<br>• अनुसंधान और विचार नेतृत्व पहलों का नेतृत्व करने का सिद्ध अनुभव.<br>• साइबर सुरक्षा रणनीतियाँ बनाने और उन्हें लागू करने का अनुभव.<br>• सुरक्षा प्रौद्योगिकी में महारत, जिसमें फायरवॉल, घुसपैठ का पता लगाने/रोकने वाले सिस्टम (IDS/IPS), SIEM और एंडपॉइंट प्रोटेक्शन शामिल हैं.<br>• थ्रेट इंटेलिजेंस प्लेटफॉर्म और टूल में दक्षता.<br>• साइबर फोरेंसिक और घटना के समय की जाने वाली कार्रवाई की प्रक्रियाओं की जानकारी.<br>• किसी नए खतरे से संगठन पर पड़ने वाले असर की संभावना का विश्लेषण करना और कमज़ोरियों की पहचान करना.<br>• खतरों को कम करने और सुधार के प्रयासों को असरदार बनाने के लिए बिज़नेस को रिपोर्ट और सुझाव देना.<br>• एक व्यापक साइबर सुरक्षा रणनीति बनाने और उसे लागू करने की क्षमता.<br>• जटिल सुरक्षा समस्याओं का विश्लेषण करने और प्रभावी समाधान विकसित करने की क्षमता.<br>• साइबर सुरक्षा जोखिमों का आकलन करने, उन्हें कम करने और उनका प्रबंधन करने की क्षमता.<br>• साइबर सुरक्षा घटनाओं के प्रबंधन और उन पर प्रतिक्रिया देने का अनुभव.<br>• संबंधित साइबर सुरक्षा मानकों, नियमों और सर्वोत्तम कार्यप्रणालियों का ज्ञान. |

| **पद संख्या/पद नाम** | **4 - उप प्रबंधक – एआई विशेषज्ञ** |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:** कंप्यूटर साइंस/कंप्यूटर साइंस एवं इंजीनियरिंग/डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/सॉफ्टवेयर इंजीनियरिंग/सूचना प्रौद्योगिकी /इलेक्ट्रॉनिक्स/इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में बी.टेक/बी.ई. या ऊपर निर्दिष्ट विषयों में कम से कम 50% अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से कंप्यूटर साइंस/ कंप्यूटर साइंस एवं इंजीनियरिंग/ सूचना प्रौद्योगिकी/ डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में समतुल्य डिग्री. |

| | |
|---|---|
| **अन्य योग्यता (31.07.2026 तक)** | **प्रोफेशनल सर्टिफ़िकेशन:**<br>1. ISACA यूएसए से एडवांस्ड एआई ऑडिट (AAIA)<br>2. ISACA यूएसए से एडवांस्ड एआई सिक्योरिटी मैनेजमेंट (AAISM)<br>3. ISACA यूएसए से एडवांस्ड एआई रिस्क (AAIR)<br>4. AWS सर्टिफ़ाइड एआई प्रैक्टिशनर<br>5. गूगल क्लाउड प्रोफेशनल एमएल इंजीनियर<br>6. आईबीएम एआई इंजीनियरिंग प्रोफेशनल सर्टिफ़िकेट |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:** सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव. इन 4 वर्षों में से, 2 वर्ष का अनुभव इन कामों में होना चाहिए: एमएल/ डीप लर्निंग मॉडल डिज़ाइन करना/ वर्कफ़्लो मैपिंग/ GenAI/आरएजी पाइपलाइन डिप्लॉय करना/ सुरक्षित एपीआई डिप्लॉयमेंट/ एडब्ल्यूएस सेजमेकर, गूगल क्लाउड वर्टेक्स एआई या माइक्रोसाफ्ट एज्योर एमएल जैसे क्लाउड एमएल सूट का अनुभव/ टेन्सरफ्लो, पाइटॉर्च, साइकिट-लर्न, पैंडास, एक्सजीबूस्ट, हगिंग फेस, लैंग चेन, ओपन एआई एपीआई, अपाचे स्पार्क, पाइथन, प्रॉम्प्ट इंजीनियरिंग, फाइन ट्यूनिंग जैसी लाइब्रेरीज़ में महारत.<br>**प्राथमिकता:** एआई से जुड़े क्षेत्र में अनुभव को प्राथमिकता दी जाएगी.<br><br>**शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • **एकीकरण, परीक्षण और परिनियोजन:** एकीकरण की ज़रूरतों को समझना, आंतरिक तकनीकी टीमों के साथ तालमेल बिठाना, टेस्ट केस तैयार करना, डेटा फ़्लो और सिस्टम कम्पैटिबिलिटी को सत्यापित करना. एआई सिस्टम को रियल-टाइम में मॉनिटर करना और उनमें आने वाली दिक्कतों को ठीक करना.<br>• **एआई/एमएल डेवलपमेंट और इष्टतमीकरण:** एआई एल्गोरिदम और SLMs, LLMs, CNNs, GANs, एजेंट्स, हार्नेस, गार्डरेल्स जैसे मॉडलों को विकसित करना और लागू करना. बड़े डेटासेट का विश्लेषण और पूर्व-प्रसंस्करण करना. मॉडल के प्रदर्शन का मूल्यांकन करना और बेहतर परिणामों के लिए उसे फ़ाइन-ट्यून करना. डेटा फ़्लो और इन्फ़रेंस के लिए हार्डवेयर और सॉफ़्टवेयर डिज़ाइन के ज़रिए मॉडल को ऑप्टिमाइज़ करना.<br>• **डेटा, क्लाउड और इंफ़्रास्ट्रक्चर:** हैडूप और स्पार्क जैसी बिग डेटा टेक्नोलॉजीज़ के साथ काम करना. एडब्ल्यूएस, गूगल क्लाउड या एज्योर जैसे क्लाउड प्लेटफ़ॉर्म का इस्तेमाल करना. प्रशिक्षण, फ़ाइन-ट्यूनिंग और परिनियोजन के लिए हार्डवेयर की आवश्यकताओं का प्रबंध करना.<br>• **सुरक्षा और अनुपालन:** प्रतिकूल एआई टूल्स का इस्तेमाल करके एआई मॉडल का सुरक्षा आकलन करना. मॉडल पॉइज़निंग, बायस और संवेदनशीलताओं की पहचान करना. एथिकल बातों और संबंधित नियमों का पालन सुनिश्चित करना.<br>• **अनुसंधान, दस्तावेजीकरण और सहयोग:** एआई/ एमएल में अनुसंधान करना और प्रकाशित कार्य का रिकॉर्ड बनाए रखना. एआई मॉडल और सॉल्यूशन के लिए दस्तावेजीकरण तैयार करना और उसे बनाए रखना. कोड रिव्यू में हिस्सा लेना और टीम के साथ जानकारी शेयर करने में योगदान देना. Git जैसे वर्ज़न कंट्रोल सिस्टम का इस्तेमाल करना.<br>• **तकनीकी कौशल और जानकारी:** पाइथन, जावा या C++ जैसी प्रोग्रामिंग भाषाओं में महारत. एआई / एमएल फ्रेमवर्क और लाइब्रेरी का अनुभव. एआई और मशीन लर्निंग में उद्योग की प्रवृत्तियों और नई प्रगति के बारे में अपडेट रहना. |

| पद संख्या/पद नाम | **5 - उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ** |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:**<br>कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सॉफ्टवेयर इंजीनियरिंग/ इंफॉर्मेशन टेक्नोलॉजी/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में बी.टेक/ बी.ई. या ऊपर निर्दिष्ट विषयों में कम से कम **50%** अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से कंप्यूटर साइंस/ कंप्यूटर साइंस एवं इंजीनियरिंग/ सूचना प्रौद्योगिकी/ डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में समतुल्य डिग्री.<br>**प्राथमिकता:**<br>**साइबर सुरक्षा या सूचना प्रौद्योगिकी में एडवांस्ड डिग्री को प्राथमिकता दी जाएगी.** |
| **अन्य योग्यता (31.07.2026 तक)** | **अधिमान्य प्रमाणन:**<br>आईएसओ 27001/ CISSP/ CISA/ CRISC/ CISM/ CCSP/ GDPR/ DPDPA/ साइबर सुरक्षा गवर्नेंस, जोखिम और अनुपाल में एडवांस्ड सर्टिफ़िकेशन या पोस्ट-ग्रेजुएट डिप्लोमा. |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:**<br>न्यूनतम अनुभव: साइबर सुरक्षा या सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव.<br>**प्राथमिकता:**<br>• साइबर सुरक्षा अनुपालन भूमिकाओं में योग्यता के बाद न्यूनतम 2 वर्ष का अनुभव.<br>• बैंकिंग और वित्तीय उद्योग के विनियमन और अनुपालन अपेक्षाओं की अच्छी समझ, जैसे आरबीआई का साइबर सुरक्षा फ्रेमवर्क, सेबी के साइबर सुरक्षा दिशानिर्देश/ आईएसओ 27001/ NIST/ SOC2/ PCI DSS/ GDPR/ DPDPA/ भारत का NCIIPC/ CERT-In फ्रेमवर्क.<br>• बीएफएसआई क्षेत्र में साइबर सुरक्षा जोखिम और उससे निपटने के तरीकों की समझ. |

| | |
|---|---|
| | **शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • साइबर सुरक्षा से जुड़े नियमों, मानकों और फ्रेमवर्क्स (ISO 27001/ NIST/SOC2/PCIDSS, आदि) की अच्छी जानकारी.<br>• अनुपालन निगरानी, लेखापरीक्षा प्रबंधन और नीति गवर्नेंस का अनुभव.<br>• आईटी जनरल कंट्रोल्स (ITGC) और जोखिम प्रबंधन ढांचे की जानकारी.<br>• उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल<br>• अलग-अलग विभागों की टीमों और बाहरी विनियामकों के साथ मिलकर काम करने की क्षमता.<br>• विनियमों और उद्योग मानकों में होने वाले बदलावों की जानकारी रखना.<br>• संबंधित नियमों और अनुपालन ढांचे की गहरी समझ.<br>• उत्कृष्ट संप्रेषण और अंतर-व्यक्तिगत कौशल (लिखित और मौखिक).<br>• स्वतंत्र रूप से और टीम के साथ काम करने की क्षमता.<br>• जोखिम प्रबंधन या उससे जुड़े क्षेत्र में अनुभव होना एक अतिरिक्त लाभ होगा. |

| **पद संख्या/पद नाम** | **6 - उप प्रबंधक – साइबर सुरक्षा एनालिस्ट** |
|---|---|
| **मूल योग्यता (31.07.2026 तक)** | **अनिवार्य:**<br>कंप्यूटर साइंस/ कंप्यूटर साइंस और इंजीनियरिंग/ सॉफ्टवेयर इंजीनियरिंग/ इंफॉर्मेशन टेक्नोलॉजी/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स और संचार इंजीनियरिंग में बी.टेक/ बी.ई. या ऊपर निर्दिष्ट विषयों में **कम से कम 50%** अंकों के साथ समतुल्य डिग्री.<br>या<br>एमसीए<br>या<br>कंप्यूटर साइंस/ कंप्यूटर साइंस एवं इंजीनियरिंग/ सूचना प्रौद्योगिकी/ डेटा साइंस एवं आर्टिफिशियल इंटेलिजेंस/ सॉफ्टवेयर इंजीनियरिंग/ इलेक्ट्रॉनिक्स/ इलेक्ट्रॉनिक्स एवं संचार इंजीनियरिंग में एम.टेक/ एमएसई या ऊपर निर्दिष्ट विषयों में समतुल्य डिग्री.<br>(भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से) |
| **अन्य योग्यता (31.07.2026 तक)** | **अधिमान्य प्रमाणन:**<br>आईएसओ 27001/ CISSP/ CISA/ CRISC/ CISM/ CCSP/ GDPR/ DPDPA/ साइबर सुरक्षा पॉलिसी/ अनुपाल में एडवांस्ड सर्टिफ़िकेशन या पोस्ट-ग्रेजुएट डिप्लोमा. |
| **कार्य अनुभव (मूल योग्यता के बाद) (31.07.2026 तक)** | **अनिवार्य:**<br>न्यूनतम अनुभव: साइबर सुरक्षा या सूचना प्रौद्योगिकी के क्षेत्र में योग्यता के बाद 4 वर्ष का अनुभव.<br>**प्राथमिकता:**<br>आईटी सुरक्षा नीति/साइबर सुरक्षा नीति के विकास, तकनीकी लेखन, या गवर्नेंस, जोखिम और अनुपालन (GRC) भूमिकाओं में योग्यता के बाद न्यूनतम 2 वर्ष का अनुभव. ISO 27001/NIST/SOC2/PCI DSS/GDPR/DPDPA/भारत के NCIIPC/CERT-In फ्रेमवर्क जैसे मानकों या फ्रेमवर्क को डॉक्यूमेंट करने का अनुभव. पॉलिसी एडवोकेसी और प्रसार के क्षेत्रों में अनुभव. उत्कृष्ट मौखिक और लिखित संप्रेषण कौशल.<br>**शिक्षण एवं प्रशिक्षण अनुभव को पात्रता में नहीं गिना जाएगा.**<br>**नोट:** उम्मीदवारों को अद्यतन और पूर्ण अनुभव प्रमाण पत्र प्रस्तुत करना आवश्यक है, जिसमें स्पष्ट रूप से दर्शाया गया हो:<br>(i) नौकरी की प्रकृति,<br>(ii) अनुभव की तिथियां और अवधि,<br>(iii) स्तर/पद,<br>(iv) नियोक्ता(ओं) द्वारा सौंपी गई जिम्मेदारियाँ आदि.<br>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:** | • मज़बूत विश्लेषणात्मक और अनुसंधान कौशल, साथ ही जटिल नीतियों और प्रवृत्तियों की व्याख्या करने की क्षमता.<br>• मुख्य हितधारकों के साथ संबंध बनाने और बनाए रखने तथा नीतिगत निर्णयों को प्रभावित करने की सिद्ध क्षमता.<br>• मज़बूत सहयोग और अंतर-व्यक्तिगत कौशल के साथ टीम के खिलाड़ी.<br>• सोच और लेखन में व्यवस्थित, क्रमबद्ध और संरचित.<br>• विविध प्रकार के लोगों के सामने जटिल जानकारी को स्पष्ट और संक्षिप्त रूप में प्रस्तुत करने की क्षमता.<br>• इस पद के लिए तकनीकी विशेषज्ञता, नीति की जानकारी और प्रभावी ढंग से एडवोकेसी करने के कौशल के संयोजन की आवश्यकता है.<br>• एडवोकेसी में कई तरह की गतिविधियाँ शामिल हैं, जैसे जन-जागरूकता अभियान, एक्सपर्ट ब्रीफ़, विधायी लॉबिंग, और विशिष्ट नीतिगत परिणामों के लिए नीति निर्माताओं के साथ जुड़ना.<br>• साइबर सुरक्षा से जुड़ी संवेदनशीलताओं को नियंत्रित करने और साइबर-केंद्रित नीतियां व रणनीतियां बनाने का व्यावहारिक अनुभव और कौशल; साथ ही, नवीनतम विनियामक और तकनीकी मानकों के अनुसार उन्हें प्रभावी ढंग से नीति के रूप में लागू करना.<br>• साइबर नीतियों को बनाना और लागू करना.<br>• नीति लागू करने की प्रक्रिया की समझ. |

**महत्वपूर्ण बिंदु:**

1. विभिन्न पदों के लिए निर्धारित शैक्षणिक योग्यता न्यूनतम है. उम्मीदवार को निर्दिष्ट तिथियों तक मूल योग्यता के बाद और प्रासंगिक पूर्णकालिक अनुभव होना चाहिए.
2. **नियोक्ता से प्राप्त प्रासंगिक 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 निर्दिष्ट नहीं करते हैं, तो वहाँ 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.** | **डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब** | **कार्य प्रोफ़ाइल:**<br>सेंटर ऑफ एक्सीलेंस (CoE) के अंतर्गत नवोन्मेषण और सिमुलेशन लैब का नेतृत्व करना, और प्रयोग, प्रोटोटाइपिंग व व्यावहारिक शोध की संस्कृति को बढ़ावा देना. इस भूमिका का मुख्य उद्देश्य रणनीतिक नवोन्मेषण को आगे बढ़ाना, वास्तविक दुनिया की साइबर सुरक्षा और टेक्नोलॉजी चुनौतियों का सिमुलेशन करना, और संगठन की डिजिटल व साइबर क्षमताओं को भविष्य के लिए तैयार करने हेतु नए समाधानों के विकास और परीक्षण में तेज़ी लाना है.<br><br>**मुख्य दायित्व क्षेत्र (केआरए):**<br>**मुख्य जिम्मेदारियां:**<br>**नवोन्मेषण रणनीति:**<br>• सेंटर ऑफ एक्सीलेंस (CoE) के लक्ष्यों और संगठन के समग्र साइबर सुरक्षा उद्देश्यों के अनुरूप एक व्यापक नवोन्मेषण रणनीति तैयार करना.<br>**नवोन्मेषण लैब:**<br>• अत्याधुनिक सुविधाओं को सुनिश्चित करने के लिए नवोन्मेषण और अनुसंधान लैब के डिज़ाइन को सक्षम बनाना.<br>• अनुसंधान और नवोन्मेषण गतिविधियों के लिए एक ढांचा तैयार करना, जिसमें इंफ्रास्ट्रक्चर को सक्षम बनाना, परिचालनात्मक मॉडल, परिणम मापन आदि शामिल हों.<br>• लैब के कार्यान्वयन और संचालन के लिए रणनीतिक और परिचालनात्मक संबंध बनाना.<br>**परिचालनात्मक उत्कृष्टता:**<br>• यह सुनिश्चित करना कि लैब कुशलतापूर्वक काम करे, जिसमें संसाधनों का प्रभावी आवंटन और परियोजना प्रबंधन के तरीके शामिल हों.<br>• अनुसंधान पहलों और नवोन्मेषण परियोजनाओं की प्रगति की निगरानी करना और रिपोर्ट करना.<br>• लैब के बजट का प्रबंधन करना और अधिकतम प्रभाव के लिए संसाधनों का सही इस्तेमाल सुनिश्चित करना.<br>**नवोन्मेषण और समाधान विकास:**<br>• अनुसंधान के परिणामों को व्यावहारिक साइबर सुरक्षा समाधानों और रणनीतियों में बदलना.<br>• नई प्रौद्योगिकियों और कार्यप्रणालियों का मूल्यांकन करना और उन्हें मौजूदा ढांचे में शामिल करना.<br>• नई प्रौद्योगिकियों को प्रदर्शित करने के लिए प्रोटोटाइप/टूलकिट और प्रूफ–ऑफ–कांसेप्ट डेमोंस्ट्रेशन के विकास को बढ़ावा देना.<br>**उभरती प्रौद्योगिकियां:**<br>• सीओई के लिए संभावित उपयोग और अवसरों की पहचान करने के लिए एआई, मशीन लर्निंग, ब्लॉकचेन और क्वांटम कंप्यूटिंग जैसी उभरती साइबर सुरक्षा प्रौद्योगिकियों पर अनुसंधान और मूल्यांकन करना.<br>**ज्ञान साझा करना:**<br>• सीओई में ज्ञान साझा करने और सहयोग की संस्कृति को बढ़ावा देना, जिससे उत्कृष्ट पद्धतियों, अनुसंधान परिणामों और सीखे गए अनुभवों को आसानी से प्रसारित किया जा सके.<br>**बाहरी जुड़ाव:**<br>• उद्योग के विशेषज्ञों, अनुसंधान संस्थानों और टेक्नोलॉजी वेंडर्स जैसे बाहरी हितधारकों के साथ संबंध बनाना और बनाए रखना, ताकि नवीनतम प्रवृत्तियों की जानकारी रहे और सहयोग को बढ़ावा मिले.<br>**प्रतिभा विकास:**<br>• सेंटर ऑफ एक्सीलेंस (CoE) के भीतर प्रतिभा की पहचान करना और उसे निखारना; नवोन्मेषण और साइबर सुरक्षा से जुड़े क्षेत्रों में पेशेवर विकास और वृद्धि के अवसर देना.<br>**कार्य–निष्पादन मापन:**<br>• नवोन्मेषण पहलों की प्रभावशीलता और सीओई के कुल प्रभाव को मापने के लिए मुख्य कार्य–निष्पादन संकेतक (KPIs) तय करना और उन्हें ट्रैक करना.<br>**सुरक्षा की स्थिति को बेहतर बनाना:**<br>नए और नवोन्मेषी समाधानों और बेहतरीन तौर–तरीकों को अपनाकर संगठन की सुरक्षा की स्थिति को लगातार बेहतर बनाना. |
| **2.** | **डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक–केंद्रित पहल** | **कार्य प्रोफ़ाइल:**<br>संगठन के लक्ष्यों के अनुसार नागरिकों पर केंद्रित पहलों का नेतृत्व, डिज़ाइन और कार्यान्वयन करना, ताकि यह सुनिश्चित हो सके कि सेवाएँ सुलभ, समावेशी, कुशल और प्रभावशाली हों. इस भूमिका के लिए रणनीतिक सोच, हितधारकों के साथ मजबूत जुड़ाव, कार्यक्रम प्रबंधन क्षमताएँ और डिजिटल व भौतिक शासन पहलों में नागरिकों की ज़रूरतों की गहरी समझ की आवश्यकता है. सेंटर ऑफ एक्सीलेंस (CoE) के तहत नागरिकों पर केंद्रित कार्यक्रमों के लिए विज़न और रोडमैप तैयार करना और उनका नेतृत्व करना.<br><br>**मुख्य दायित्व क्षेत्र (केआरए):**<br>➢ साइबर सुरक्षा रणनीतियाँ विकसित और कार्यान्वित करना:<br>• इसमें नागरिकों को साइबर खतरों, जैसे साइबर अपराध, ऑनलाइन धोखाधड़ी और डेटा की चोरी से बचाने के लिए योजनाएँ बनाना और उन्हें लागू करना शामिल है.<br>➢ कार्यक्रम प्रबंधन:<br>• नागरिकों पर केंद्रित परियोजनाओं की योजना, कार्यान्वयन और डिलीवरी की देखरेख करना और यह सुनिश्चित करना कि वे समय पर और बजट के भीतर पूरी हों.<br>• पहलों के सुचारू एकीकरण और कार्यान्वयन को सुनिश्चित करने के लिए विभिन्न विभागों और टीमों के बीच समन्वय करना.<br>• परियोजना की प्रगति की निगरानी करना, संभावित जोखिमों और मुद्दों की पहचान करना और जोखिम कम करने की रणनीतियों को लागू करना.<br>➢ साइबर जागरूकता और साक्षरता को बढ़ावा देना:<br>• नागरिकों को ऑनलाइन सुरक्षा, डिजिटल नागरिकता और ज़िम्मेदार ऑनलाइन व्यवहार के बारे में शिक्षित करना अत्यंत आवश्यक है.<br>➢ सुरक्षित डिजिटल सेवाओं तक पहुँच सुनिश्चित करना:<br>• सभी नागरिकों के लिए सरकारी सेवाओं को सुलभ और सुरक्षित बनाने की दिशा में काम करना, चाहे उनकी तकनीकी जानकारी कैसी भी हो. |

| | | |
|---|---|---|
| | | ➢ सहयोग को बढ़ावा देना:<br>• एक सुरक्षित ऑनलाइन माहौल बनाने के लिए कानून लागू करने वाली एजेंसियों, टेक्नोलॉजी कंपनियों और गैर–लाभकारी संगठनों जैसे विभिन्न हितधारकों के साथ मिलकर काम करना.<br>➢ टीम का नेतृत्व करना:<br>• पहल के लक्ष्यों को हासिल करने के लिए साइबर सुरक्षा पेशेवरों की टीम का प्रबंधन और मार्गदर्शन करना.<br>➢ तकनीकी विशेषज्ञता:<br>• नागरिक–केंद्रित समाधान डिज़ाइन करने और उन्हें लागू करने के लिए तकनीकी मार्गदर्शन और सहायता देना.<br>• इंटरनेट ऑफ थिंग्स (IoT), स्मार्ट इंफ्रास्ट्रक्चर, साइबर सुरक्षा और ई–गवर्नेंस जैसे क्षेत्रों में नई प्रौद्योगिकियों और प्रवृत्तियों के बारे में अपडेट रहना.<br>• नागरिकों के इस्तेमाल वाले विशिष्ट एप्लिकेशन के लिए सही प्रौद्योगिकियों का मूल्यांकन करना और उनकी सिफारिश करना. |
| **3.** | **उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा** | **कार्य प्रोफ़ाइल:**<br>इस भूमिका में अनुसंधान पहल का नेतृत्व करना, विचार–नेतृत्व वाला कंटेंट तैयार करना और संगठन के अंदर व बाहर साइबर सुरक्षा में उत्कृष्टता की संस्कृति को बढ़ावा देना शामिल है. यह भूमिका संगठन की साइबर सुरक्षा रणनीति और कामकाज की देखरेख और प्रबंधन करती है, जिसमें खतरों का पता लगाने, घटना पर प्रतिक्रिया देने और इंटेलिजेंस इकट्ठा करने पर ध्यान दिया जाता है. इसमें टीम बनाना और उसका प्रबंधन करना, सुरक्षा नीतियां और प्रक्रियाएं विकसित करना और लागू करना, खतरे की इंटेलिजेंस का विश्लेषण करना और साइबर घटनाओं पर प्रतिक्रिया देना शामिल है. वे उभरते साइबर सुरक्षा खतरों और सर्वोत्तम प्रथाओं पर संगठन के नज़रिए को आकार देने और व्यापक साइबर सुरक्षा चर्चा में योगदान देने के लिए ज़िम्मेदार होते हैं.<br><br>**मुख्य दायित्व क्षेत्र (केआरए):**<br>➢ रणनीतिक आयोजना:<br>• वैश्विक साइबर डिफेंस और इंटेलिजेंस प्रोग्राम को तय करना और बेहतर बनाना.<br>• सीओई की साइबर डिफेंस और इंटेलिजेंस रणनीति बनाना और उसे लागू करना, साथ ही इसे संगठन के कुल कारोबारी लक्ष्यों के साथ जोड़ना.<br>➢ थ्रेट इंटेलिजेंस और साइबर डिफेंस:<br>• खतरों का असरदार तरीके से पता लगाना, घटनाओं पर तुरंत कार्रवाई करना और कमज़ोरियों का प्रबंधन सुनिश्चित करना.<br>• साइबर सुरक्षा से जुड़े खतरों, घटनाओं और उनसे निपटने की योजनाओं के बारे में वरिष्ठ प्रबंधन, कारोबारी इकाइयों और अन्य हितधारकों के साथ प्रभावशाली ढंग से बातचीत करना.<br>• नए खतरों और कमज़ोरियों की पहचान करने के लिए अलग–अलग स्रोतों से मिली थ्रेट इंटेलिजेंस की निगरानी और विश्लेषण करना और उसे आगे पहुंचाना.<br>• साइबर घटनाओं के मूल कारणों और हमलावरों के तरीकों का पता लगाने के लिए फोरेंसिक जांच करना.<br>➢ साइबर डिफेंस:<br>• उन्नत मैलवेयर और फोरेंसिक कौशल<br>• मैलवेयर और फोरेंसिक लैब को डिज़ाइन करना और उसे लागू करना.<br>➢ सुरक्षा आर्किटेक्चर:<br>• संगठन की डिजिटल परिसंपत्तियों की सुरक्षा के लिए मज़बूत सुरक्षा आर्किटेक्चर और सिस्टम डिज़ाइन करना, लागू करना और उन्हें बनाए रखना.<br>➢ खतरों का पता लगाना और उनसे बचाव:<br>• अलग–अलग टूल्स और प्रौद्योगिकियों का इस्तेमाल करके संभावित खतरों के लिए माहौल पर नज़र रखना और बचाव के उपाय लागू करना.<br>➢ घटना पर प्रतिक्रिया (इंसिडेंट रिस्पॉन्स):<br>• घटना पर प्रतिक्रिया देने की योजनाओं और प्रक्रियाओं को तय करना और उन्हें बनाए रखना, साथ ही साइबर सुरक्षा से जुड़ी घटनाओं पर प्रतिक्रिया का नेतृत्व करना.<br>➢ साइबर सुरक्षा रणनीतियाँ बनाना और लागू करना:<br>• इसमें नागरिकों को साइबर खतरों (जैसे साइबर क्राइम, ऑनलाइन धोखाधड़ी और डेटा ब्रीच) से बचाने के लिए योजनाएँ बनाना और उन्हें लागू करना शामिल है.<br>➢ कार्यक्रम प्रबंधन:<br>• नागरिकों पर केंद्रित परियोजनाओं की योजना बनाना, उन्हें लागू करना और उनकी डिलीवरी की देखरेख करना, ताकि वे समय पर और बजट के अंदर पूरे हों.<br>• अलग–अलग विभागों और टीमों के बीच तालमेल बिठाना ताकि पहलों को आसानी से जोड़ा और लागू किया जा सके.<br>• परियोजना की प्रगति की निगरानी करना, संभावित जोखिमों और समस्याओं की पहचान करना और उनसे निपटने की रणनीतियाँ लागू करना.<br>➢ साइबर जागरूकता और साक्षरता को बढ़ावा देना:<br>• नागरिकों को ऑनलाइन सुरक्षा, डिजिटल नागरिकता और ज़िम्मेदार ऑनलाइन व्यवहार के बारे में शिक्षित करना बहुत ज़रूरी है.<br>➢ सुरक्षित डिजिटल सेवाओं तक पहुँच सुनिश्चित करना:<br>• सभी नागरिकों के लिए सरकारी सेवाओं को सुलभ और सुरक्षित बनाने के लिए काम करना, चाहे उनकी तकनीकी जानकारी कैसी भी हो.<br>➢ सहयोग को बढ़ावा देना:<br>• एक सुरक्षित ऑनलाइन माहौल बनाने के लिए कानून लागू करने वाली एजेंसियों, टेक्नोलॉजी कंपनियों और गैर–लाभकारी संगठनों जैसे विभिन्न हितधारकों के साथ मिलकर काम करना. |
| **4.** | **उप प्रबंधक – एआई विशेषज्ञ** | **कार्य प्रोफ़ाइल:**<br>1. एआई/एमएल विकास और एकीकरण: एआई/ एनालिटिक्स मॉडल, डैशबोर्ड, पीओसी और एलएलएम एजेंट जैसे ऑटोनॉमस टूल्स के एकीकरण परीक्षण में सहायता करना. एसएनएट, जीएएन आदि को प्रशिक्षित करना और कार्य–प्रवाह स्वचालन के लिए डेटासेट तैयार करना.<br>2. एआई सुरक्षा नियंत्रण और गवर्नेंस: एआई विकास, परीक्षण, परिनियोजन और संचालन के लिए सुरक्षा नियंत्रण तय करना. मॉडल की अखंडता, प्रमाणिकता, वर्ज़निंग, प्रूवेंस नियंत्रण और केआरआई/ केपीआई स्थापित करना. एंटरप्राइज़ फ्रेमवर्क के साथ नियंत्रणों को मैप करना और विनियामक अनुपालन सुनिश्चित करना.<br>3. जोखिम और खतरे का आकलन: फ़ाउंडेशन मॉडल, ओपन–सोर्स मॉडल, थर्ड–पार्टी एआई सर्विस और होस्टिंग/ इनफ़रेंस इंफ्रास्ट्रक्चर से जुड़े जोखिमों का आकलन करें. एआई सुरक्षा से जुड़ी घटनाओं के लिए एआई रेड टीमिंग, एडवर्सरियल टेस्टिंग और आरसीए संचालित करना.<br>4. डेटा गोपनीयता और सुरक्षा: एआई सिस्टम में संवेदनशील/ विनियमित डेटा को सुरक्षित रखना. एनॉनिमाइज़ेशन, टोकनाइज़ेशन, मास्किंग और गोपनीयता बढ़ाने वाली तकनीकों का मूल्यांकन करना. प्राइवेसी/ गोपनीयता से जुड़े जोखिमों के लिए एआई समाधानों की समीक्षा करना.<br>5. इंफ्रास्ट्रक्चर और कार्यभार सुरक्षा: कंटेनर, कुबेरनेट्स, GPU और क्लाउड–नेटिव प्लेटफ़ॉर्म पर एआई कार्यभार को सुरक्षित करना. मॉडल होस्टिंग एनवायरनमेंट और सर्विंग इंफ्रास्ट्रक्चर का मूल्यांकन करना.<br>6. गवर्नेंस, रिपोर्टिंग और हितधारक जुड़ाव: वरिष्ठ प्रबंधन के समक्ष एआई से जुड़े जोखिम प्रस्तुत करना, एआई गवर्नेंस समिति और आर्किटेक्चर बोर्ड में भाग लेना. डैशबोर्ड बनाना, ऑडिट में मदद करना और उभरते एआई/ एमएल खतरों को ट्रैक करना.<br>7. प्रोक्योरमेंट, आपूर्ति श्रृंखला और अंगीकरण: एआई उत्पाद के लिए प्रोक्योरमेंट/ ऑनबोर्डिंग समीक्षाओं में मदद करना. ओपन–सोर्स एआई कंपोनेंट और आपूर्ति श्रृंखला से जुड़े जोखिमों की समीक्षा करना. कर्मचारियों के लिए सुरक्षित जेनरेटिव एआई के इस्तेमाल के संबंध में दिशा–निर्देश तैयार करना. |

| | | |
|---|---|---|
| | | **मुख्य दायित्व क्षेत्र (केआरए):**<br>1. एआई/ एमएल विकास और एमएल ऑपरेशन्स: कार्यप्रवाह के स्वचालन के लिए एसएलएम, एलएलएम, सीएनएन और जीएएन को ट्रेन, फ़ाइन-ट्यून और परिनियोजित करना. आरएजी पाइपलाइन, एम्बेडिंग और डेटा रिपॉजिटरी बनाना. सीआई/ सीडी, वर्ज़निंग, मॉनिटरिंग और री-ट्रेनिंग का इस्तेमाल करके मॉडल को ऑपरेशनल बनाना और प्रदर्शन/लागत के लिए इष्टतम बनाना.<br>2. एजेंटिक सिस्टम और एकीकरण: ऐसे स्वायत्त एलएलएम एजेंट/ हार्नेस डिज़ाइन करना जो समग्र कार्य प्रवाह का प्रबंध करें. एआई मॉडल, डैशबोर्ड और पीओसी के परीक्षण में मदद करना और मौजूदा सिस्टम, एपीआई, प्लगइन और थर्ड-पार्टी इंटीग्रेशन के साथ सुसंगतता सुनिश्चित करना.<br>6. एआई सुरक्षा गवर्नेंस और फ्रेमवर्क: पूरे संगठन के लिए एआई/ एलएलएम सुरक्षा गवर्नेंस फ्रेमवर्क और सुरक्षित विकास मानक बनाना और उसे लागू करना. डेवलपमेंट, टेस्टिंग, डिप्लॉयमेंट और ऑपरेशन्स के दौरान मॉडल की अखंडता, प्रामाणिकता, वर्ज़निंग और प्रोवेनेंस के लिए कंट्रोल बनाना.<br>4. जोखिम आकलन और थ्रेट मॉडलिंग: फ़ाउंडेशन मॉडल, ओपन-सोर्स मॉडल, थर्ड-पार्टी एआई सर्विस और कंटेनर/ कुबेरनेट/ GPU/ क्लाउड पर वर्कलोड के लिए रिस्क का आकलन करना. प्रॉम्प्ट इंजेक्शन, जेलब्रेक, मॉडल पॉइज़निंग और डेटा लीक के लिए थ्रेट मॉडलिंग करना. एडवर्सरियल टेस्टिंग और रेड टीमिंग करना.<br>5. डेटा गोपनीयता, अनुपालन और गार्डरेल्स: एनोनिमाइज़ेशन, टोकनाइज़ेशन, मास्किंग और पीएचई टेक्नोलॉजी के ज़रिए संवेदनशील/ विनियमित डेटा को सुरक्षित करना. आरएजी पाइपलाइन, वेक्टर डीबी और नॉलेज रिपॉज़िटरी को सुरक्षित करना. एआई गार्डरेल्स, कंटेंट फ़िल्टरिंग और गलत इस्तेमाल को रोकने के उपाय लागू करें. आरबीआई, सर्ट-इन, डीपीडीपी अधिनियम, आईएसओ 42001, एनआईएसटी एआई आरएमएफ और अन्य नियमों का पालन सुनिश्चित करना.<br>6. निगरीन, घटना पर प्रतिक्रिया और हितधारक जुड़ाव: एआई ऐप्स में गड़बड़ियों, गलत इस्तेमाल और सुरक्षा से जुड़ी घटनाओं की निगरानी करें. गलत इस्तेमाल का पता लगाना आरसीए करने का काम करना; एआई परिसंपत्ति इन्वेंट्री और जोखिम रजिस्टर बनाए रखें. घटना पर प्रतिक्रिया/ फ़ोरेंसिक और ऑडिट में मदद करना, और वरिष्ठ प्रबंधन के समक्ष जोखिमों को पेश करना. एआई सुरक्षा के बारे में जागरूकता बढ़ाना और इंफ्रास्ट्रक्चर, डेटा, विधिक, अनुपालन और आर्किटेक्चर टीमों के साथ मिलकर काम करना. |
| **5.** | **उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ** | **कार्य प्रोफ़ाइल:**<br>आईटी सुरक्षा विशेषज्ञ यह सुनिश्चित करने के लिए ज़िम्मेदार होगा कि साइबर सिक्योरिटी सेंटर ऑफ़ एक्सीलेंस (CSCoE) आंतरिक नीतियों, उद्योग के नियमों और लागू साइबर सुरक्षा मानकों का पालन करे. इस भूमिका में अनुपालन ढांचे की निगरानी करना, जोखिम का आकलन करना, नीतियां बनाना और लागू करना, और संगठन की सुरक्षा स्थिति को मज़बूत करने के लिए आंतरिक और बाहरी लेखापरीक्षकों के साथ तालमेल बिठाना शामिल है. साइबर सुरक्षा अनुपालन विशेषज्ञ सार्वजनिक क्षेत्र और उद्यम माहौल के लिए एक व्यापक साइबर सुरक्षा अनुपालन डैशबोर्ड विकसित करेगा, उसकी समीक्षा करेगा और उसे बनाए रखेगा.<br><br>**मुख्य दायित्व क्षेत्र (केआरए):**<br>**अनुपालन प्रोग्राम बनाना और लागू करना:**<br>अनुपालन से जुड़ी नीतियां, प्रक्रियाएं और प्रशिक्षण सामग्री बनाना और उन्हें बनाए रखना.<br>**लेखापरीक्षा और आकलन करना:**<br>संभावित उल्लंघनों और जोखिम वाले क्षेत्रों की पहचान करने के लिए प्रक्रियाओं, पद्धतियों और दस्तावेज़ों की नियमित रूप से समीक्षा करना.<br>**अनुपालन की निगरानी करना:**<br>नियमों और आंतरिक नियंत्रणों के पालन पर नज़र रखना और जहाँ उपयुक्त हो, अनुपालन प्रबंधन प्लेटफ़ॉर्म का इस्तेमाल करना.<br>**अनुपालन मेट्रिक्स:**<br>यह आकलन करने के लिए अनुपालन मेट्रिक्स तय करना और डिज़ाइन करना कि कोई संगठन मानकों का कितनी अच्छी तरह पालन कर रहा है.<br>**रिपोर्टिंग:**<br>नियामक संस्थाओं और आंतरिक हितधारकों को अनुपालन रिपोर्ट तैयार करके सौंपना.<br><br>**जोखिम एवं लेखापरीक्षा प्रबंधन**<br>• अनुपालन जोखिम आकलन करना और साइबर सुरक्षा प्रक्रियाओं में कमियों की पहचान करना.<br>• साइबर सुरक्षा लेखापरीक्षा के दौरान आंतरिक/बाह्य लेखापरीक्षकों के साथ समन्वय करना.<br>• अनुपालन निष्कर्षों, लेखापरीक्षा टिप्पणियों और कमजोरियों पर नज़र रखना और उनका समाधान करना.<br>• विनियामक परिवेशों का ज्ञान (विशेष रूप से आईटी सुरक्षा, साइबर सुरक्षा और संबंधित नवाचार क्षेत्रों में).<br>• साइबर सुरक्षा प्रशिक्षण और शिक्षा से जुड़ी जटिल समस्याओं को पहचानने और उन्हें हल करने की क्षमता.<br>• अलग-अलग अनुपालन आवश्यकताओं को समझने और लीडरशिप टीम के लिए अनुपालन मेट्रिक्स तैयार करने के लिए हितधारकों के साथ मिलकर काम करना.<br>• उन्नत साइबर सुरक्षा संकल्पनाओं और अद्यतन तकनीकी प्रगति और व्यवधानों की समझ.<br>• साइबर सुरक्षा और प्रशिक्षण के लिए मेट्रिक्स बनाना, उनकी समीक्षा करना और उनका प्रबंध करना.<br>• लगातार बदलते साइबर सुरक्षा परिदृश्य में अद्यतन साइबर सुरक्षा खतरों, तकनीकों और सर्वोत्तम प्रथाओं के बारे में अपडेट रहना. |
| **6.** | **उप प्रबंधक – साइबर सुरक्षा एनालिस्ट** | **कार्य प्रोफ़ाइल:**<br>साइबर सुरक्षा एनालिस्ट सार्वजनिक क्षेत्र और उद्यम परिवेश के लिए व्यापक साइबर सुरक्षा नीतियां, प्रक्रियाएं और अनुपालन दस्तावेजीकरण तैयार करेंगे, उनकी समीक्षा करेंगे और उन्हें बनाए रखेंगे. एनालिस्ट एक रणनीतिक सोच रखने वाले व्यक्ति होंगे और साक्ष्यों को काम में लाए जा सकने वाले नीतिगत बदलावों में बदलने में माहिर होंगे. वे डेटा का विश्लेषण करेंगे और पॉलिसी बनाने में मदद के लिए सबूतों पर आधारित सुझाव देंगे. इस भूमिका के लिए जटिल मुद्दों को समझने और हितधारकों के समक्ष स्पष्ट और काम में लाए जा सकने वाले सुझाव पेश करने की क्षमता की आवश्यकता है.<br>अनुसंधान, ड्राफ्टिंग और एडवोकेसी पहल. सूचना सुरक्षा और साइबर सुरक्षा से संबंधित विनियामक बदलावों, नीतिगत दस्तावेजों और सरकारी परामर्श पर नज़र रखना. संक्षिप्त विवरण, पोजीशन पेपर्स और एनालिटिकल रिपोर्ट तैयार करना. निर्णय लेने और रणनीति बनाने के लिए नीति से जुड़ी जानकारी देना. नीति से संबंधित अकादमी प्रोग्राम टीम के साथ ज्ञान-साझाकरण सत्रों का समन्वय करना.<br>वे उभरते डिजिटल सुरक्षा मुद्दों पर शोध करते हैं, नीतिगत दस्तावेजों का प्रारूप तैयार करते हैं, तकनीकी और गैर-तकनीकी टीमों के साथ सहयोग करते हैं, और संबंधित नियमों और ढांचे का पालन सुनिश्चित करते हैं. उनके काम में तकनीकी वास्तविकताओं और नीतिगत अपेक्षाओं के बीच की खाई को पाटना, और जटिल साइबर सुरक्षा संकल्पनाओं को अलग-अलग तरह के लोगों के लिए स्पष्ट दिशानिर्देशों में बदलना शामिल है.<br><br>**मुख्य दायित्व क्षेत्र (केआरए):**<br>**ज़मीनी स्तर पर काम करना:**<br>• एग्जीक्यूटिव टीम के साथ मिलकर, एक ऐसी व्यापक और कई सालों तक चलने वाली समर्थनकारी रणनीति तैयार करना और लागू करना जो सेंटर के मिशन और लक्ष्यों के अनुरूप हो.<br>• स्थानीय, राज्य और राष्ट्रीय स्तर पर कानूनी और नियामक घटनाक्रमों पर नज़र रखना और उनका विश्लेषण करना, साथ ही संगठनों को रणनीतिक मार्गदर्शन देना.<br>• यह सुनिश्चित करना कि सेंटर का एडवोकेसी का काम जानकारी पर आधारित हो और जिन समुदायों के लिए हम काम करते हैं, उनकी ज़रूरतों के प्रति संवेदनशील हो. |

**नीति निर्माण और समर्थन (एडवोकेसी):**

- रिपोर्ट, ब्रीफ़, फैक्टशीट और प्रमाण सहित उच्च-गुणवत्ता वाली और साक्ष्य आधारित नीतिगत सामग्री तैयार करने के काम की देखरेख करना.
- राष्ट्रीय, राज्य और स्थानीय स्तर पर नीतिगत निर्णयों को प्रभावित करने के लिए समर्थनकारी रणनीतियां बनाना और उन्हें लागू करना.
- सरकारी निकायों, नियामकों, उद्योग संघों और सिविल सोसाइटी के हितधारकों के साथ जुड़ना और बातचीत करना.
- परिचर्चाओं, फ़ोरमों और कार्य समूहों में CSCoE का प्रतिनिधित्व करना.
- केंद्र, राज्य और स्थानीय स्तर पर सरकारी अधिकारियों, नियामकों और नीति-निर्माताओं के साथ जुड़ने की एक व्यापक रणनीति बनाना और उसे लागू करना.
- राष्ट्रीय और अंतर्राष्ट्रीय स्तर पर उभरती साइबर सुरक्षा नीतियों और विनियमों की पहचान करना और उनका विश्लेषण करना.
- नीतिगत चर्चाओं और फ़ोरम में CSCoE का प्रतिनिधित्व करना और संगठन के विचारों और प्राथमिकताओं का समर्थन करना.
- नीतिगत ढांचों को प्रभावित करना, जिसमें डेटा सुरक्षा, इंटरनेट सुरक्षा और डिजिटल अर्थव्यवस्था के विनियमों जैसे जटिल मुद्दों पर सरकारी निकायों को सुझाव और सिफारिशें देना शामिल है.

**जोखिम आकलन और प्रबंधन:**

- CSCoE के लिए संभावित नीतिगत जोखिमों और अवसरों की पहचान करना और उनका आकलन करना.
- नीतिगत जोखिमों को कम करने और अवसरों का लाभ उठाने के लिए रणनीतियाँ बनाना और उन्हें लागू करना.
- नीतिगत घटनाक्रमों को लागू करना और उन पर नज़र रखना, साथ ही CSCoE नेतृत्व को समय-समय पर अपडेट देना.

**आंतरिक सहयोग:**

- नीतिगत मामलों पर तालमेल सुनिश्चित करने के लिए CSCoE की अनुसंधान, तकनीकी और प्रशिक्षण सहित अन्य टीमों के साथ मिलकर काम करना.
- साइबर सुरक्षा नीति की साझा समझ को बढ़ावा देने के लिए अन्य टीमों के साथ जानकारी और विशेषज्ञता साझा करना.

**रिपोर्टिंग और संचार:**

- नीति समर्थनकारी गतिविधियों और उनके परिणामों पर रिपोर्ट और ब्रीफिंग तैयार करना.
- नीतिगत घटनाक्रमों और उनके संभावित प्रभाव के बारे में आंतरिक और बाह्य हितधारकों को जानकारी देना.
- यह भूमिका जटिल विनियमों को कार्रवाई-योग्य दस्तावेंजों में बदलने पर फोकस करती है.
- नीति लेखन, जोखिम आकलन और सरकारी मानकों के अनुरूप काम करने में विशेषज्ञता दिखाना.
- विभिन्न ज़रूरतों को समझने और तकनीकी दस्तावेजीकरण तैयार करने के लिए हितधारकों के साथ मिलकर काम करना.
- वे प्रशिक्षण का पाठ्यक्रम डिज़ाइन करेंगे और उसी के अनुसार प्रशिक्षण सामग्री तैयार करेंगे.
- लगातार बदलते साइबर सुरक्षा परिदृश्य में, साइबर सुरक्षा से जुड़े नए खतरों, टेक्नोलॉजी और सर्वोत्तम प्रथाओं के बारे में अपडेट रहना.

**नीतिगत अनुसंधान और विश्लेषण:**

- संगठन या क्षेत्र से जुड़ी नीतियों और विनियमों पर गहराई से अनुसंधान करना.
- कमियों, अक्षमताओं और सुधार की गुंजाइश वाली जगहों की पहचान करने के लिए मौजूदा नीतियों का विश्लेषण करना.
- साइबर सुरक्षा, राजनीतिक, आर्थिक और सामाजिक प्रवृत्तियों के बारे में अपडेट रहना, जिनका नीति पर प्रभाव पड़ सकता है.

**नीतिगत सिफारिशें तैयार करना:**

- अनुसंधान निष्कर्षों के आधार पर स्पष्ट और साक्ष्य आधारित नीतिगत सिफारिशें तैयार करना.
- रैंसमवेयर, घटना पर प्रतिक्रिया और कमज़ोरियों का प्रबंधन जैसे क्षेत्रों से जुड़ी नई साइबर सुरक्षा नीतियों और मानकों पर अनुसंधान करना, उनका विश्लेषण करना और उनका प्रारूप तैयार करना.
- वरिष्ठ नेतृत्व या हितधारकों को नीतिगत समायोजनों या नई नीति शुरू करने के लिए काम के और व्यावहारिक सुझाव देना.
- नीतिगत अनुसंधान रिपोर्ट और ब्रीफिंग नोट्स समय पर देना.
- एडवोकेसी पेपर्स और विनियामक प्रतिक्रियाओं के लिए उच्च गुणवत्तापूर्ण इनपुट देना.

**नीति की निगरानी और मूल्यांकन:**

- नीति के असर और प्रभाव को जानने के लिए उनके लागू होने की निगरानी करना.
- नीति के परिणामों का मूल्यांकन और आकलन करना और आवश्यक होने पर समायोजन करना.
- नीतियों की प्रगति पर रिपोर्ट देना और वास्तविक दुनिया के डेटा के आधार पर सुधार के सुझाव देना.
- नेतृत्व और नीति निर्माताओं के लिए रिपोर्ट, डैशबोर्ड और प्रेजेंटेशन तैयार करना.
- यह सुनिश्चित करना कि साइबर सुरक्षा नीति कानूनी ज़रूरतों और उद्योग ढांचे जैसे NIST का पालन करती हों.

**निष्कर्शों की जानकारी देना:**

- नीतिगत विश्लेषण और सुझावों को सूचित करने के लिए साफ़ और संक्षिप्त रिपोर्ट और प्रेजेंटेशन तैयार करना.
- नीतिगत चर्चाओं, सम्मेलनों और कार्य समूहों में संगठन का प्रतिनिधित्व करना.
- साइबर सुरक्षा की जटिल संकल्पनाओं को तकनीकी और गैर-तकनीकी दोनों तरह के लोगों के लिए आसान भाषा में समझाना.

**रणनीति पहलों में मदद करना:**

- संगठन के लक्ष्यों और मूल्यों के अनुसार लंबी अवधि की नीतिगत रणनीतियाँ बनाने में मदद करना.
- नीतिगत परिवर्तन के लिए रणनीतिक ढांचा तैयार करने में योगदान देना.

**टिप्पणी: वास्तविक केआरए कार्यग्रहण करने पर सौंपा जाएगा. ऊपर वर्णित भूमिकाएं/दायित्व/कार्य रूपरेखा उदाहरण स्वरुप में हैं. ऊपर उल्लिखित दायित्वों के अलावा, बैंक द्वारा आवश्यकताओं के अनुसार समय-समय पर अन्य भूमिकाएं/ जिम्मेदारियां/ गतिविधियां/ प्रमुख इंटरैक्शन / कार्य भी सौंपे जा सकते हैं.**

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

**घ. पारिश्रमिक/ सुझाया गया पदस्थापना का स्थान:**

| क्र. सं. | पद का नाम | वार्षिक सीटीसी की ऊपरी सीमा^ (रु. लाख में) | वार्षिक सीटीसी के विभिन्न मद | संविदा अवधि $ | सुझाया गया पदस्थापना का स्थान |
|---|---|---|---|---|---|
| 1. | डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब | ऊपरी सीमा - रु. 60.00 लाख | नियत वेतन – सीटीसी का 90%<br>परिवर्ती वेतन# – सीटीसी का 10%<br>वार्षिक वेतन वृद्धि बैंड^^ – 10% तक | 3 वर्ष. बैंक के विवेक पर और परस्पर सहमत निबंधनों और शर्तों पर इसे 2 वर्ष के लिए और बढ़ाया जा सकता है (कुल कार्यकाल 5 वर्ष से अधिक नहीं होना चाहिए). | मुंबई या किसी भी प्रशासनिक आवश्यकता के मामले में भारत में कहीं भी. |
| 2. | डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक–केंद्रित पहल | | | | |
| 3. | उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा | | | | |
| 4. | उप प्रबंधक – एआई विशेषज्ञ | 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. | | **नियमित पद** | |
| 5. | उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ | | | | |
| 6. | उप प्रबंधक – साइबर सुरक्षा एनालिस्ट | | | | |

**^ वार्षिक सीटीसी बातचीत से तय की जाएगी और यह वर्तमान रोजगार में उम्मीदवारों के अनुभव और परिलब्धियों और पदस्थापना के स्थान पर निर्भर करेगी.**

**$ संविदा को किसी भी समय, बिना किसी पूर्वाग्रह के, किसी भी पक्ष की ओर से 03 महिने का नोटिस देकर या उसके बदले में 03 महिने की वेतन राशि का भुगतान/सरेंडर करने पर समाप्त किया जा सकता है.**

**^^ दूसरे वर्ष से 10% (कार्य–निष्पादन के आधार पर) की प्रस्तावित वार्षिक वेतन वृद्धि, यदि कोई है.**

**# संविदात्मक अधिकारी के कार्य–निष्पादन के आधार पर परिवर्ती वेतन संरचना निम्नानुसार होगी:**

| | |
|---|---|
| 99 से 100% | 100% |
| 97 से 98.99 % | 90% |
| 94 से 96.99% | 80% |
| 90 से 93.99% | 70% |
| 90% से कम | शून्य |

**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 प्राप्त 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. साक्षात्कार 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 स्थान दिया जाएगा

**च. साक्षात्कार के लिए कॉल लेटर:**

साक्षात्कार 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 उन्हें 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 अपनी 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 है.

iii. उम्मीदवार आवेदन को ध्यानपूर्वक भरें. आवेदन पूरी तरह से भरने के बाद ही उम्मीदवार इसे सबमिट 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 बदल कर संशोधन करने की अनुमति मात्र तीन बार तक होगी. आवेदन के पूरी तरह भर जाने पर उम्मीदवार इसे सबमिट करें और ऑनलाइन शुल्क का भुगतान करें.

iv. **उम्मीदवारों को यह सूचना दी जाती है कि वे ऑनलाइन पंजीकरण के बाद, सिस्टम निर्मित 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/- (सात सौ पचास रुपए मात्र) है 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 जनरेट होगा 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 दस्तावेज़ो 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 प्रमाणपत्र: 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)

xiii. संविदात्मक पदों के लिए सीटीसी पर बातचीत

**ब. फोटोग्राफ फाइल टाइप/साइज़:**

i. फोटोग्राफ 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 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 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 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 होंगा 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 कैपिटल 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 रिज़ोल्यूंशन, 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 प्रति 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 को फोल्डर/फाइल की लिस्टिंग कर या फिर फाइल इमेज के आइकन पर माउस को घुमाकर जांचा जा सकता है

vi. जो उम्मीदवार एमएस विन्डोज़/एमएस ऑफिस का प्रयोग करते हैं, वे आसानी से फोटो और हस्ताक्षर जेपीईजी फार्मेट में प्राप्त कर सकते हैं जो कि क्रमश: 50 केबी और 20 केबी से अधिक न होगा, 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 कराया 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 पर क्लिक करें. यदि फाइल का आकार और प्रारूप बताए अनुसार नहीं है तो इसमें त्रुटि का संदेश आएगा.

vi. दस्तावेज़ अपलोड/ सबमिट 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.** यदि फोटो या हस्ताक्षर स्पष्ट रूप से नहीं दिखें तो उम्मीदवार अपने आवेदन को संशोधित कर सकता/सकती है और अपने फोटो या हस्ताक्षर आवेदन फार्म सबमिट किए जाने से पहले फिर से अपलोड कर सकता/सकती है. **यदि फोटो पर चेहरा या हस्ताक्षर 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 सहित ऐसे उम्मीदवार 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 उसकी 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 की नियुक्ति/तैनाती बैंक की आवश्यकता के अनुसार चिकित्सकीय रूप से उपयुक्त घोषित किए जाने के अधीन है. इस तरह की नियुक्ति/तैनाती 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 कि स्थिति में बैंक की कोई जिम्मेदारी नहीं होगी.

viii. जो उम्मीदवार सरकारी/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 यदि वे किसी यात्रा व्यय की प्रतिपूर्ति के लिए पात्र होंगे, तो उन्हें उसका भुगतान नहीं किया जाएगा.

ix. चयनित होने पर उम्मीदवारों से अपेक्षा होगी कि वह नियुक्ति/तैनाती 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 ऑनलाइन आवेदन प्रस्तुत कर दें और वे अंतिम तारीख का इंतज़ार न करें, 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 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.

xi. पात्रता, साक्षात्कार आयोजित किए जाने, अन्य परीक्षाएं और चयन संबधी 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 स्थिति 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. बाहर से आने वाले उम्मीदवारों, जिन्हें शॉर्टलिस्टिंग के बाद साक्षात्कार के लिए बुलाया जा सकता है, उन्हें नीचे बताए गए अनुसार भारत में सबसे लघुतर मार्ग से हवाई यात्रा (इकोनॉमी क्लास) के खर्च की प्रतिपूर्ति की जाएगी.

| पद | प्रतिपूर्ति सीमा |
|---|---|
| 1. उप प्रबंधक – एआई विशेषज्ञ | ₹10,000 तक हवाई किराए (आने-जाने का कुल खर्च) या वास्तविक किराया, जो भी कम हो, की प्रतिपूर्ति. |
| 2. उप प्रबंधक – आईटी सुरक्षा विशेषज्ञ | |
| 3. उप प्रबंधक – साइबर सुरक्षा एनालिस्ट | |
| 1. डिप्टी वाइस प्रेसिडेंट (DVP) – साइबर इनोवेशन एवं सिमुलेशन लैब | ₹15,000 तक हवाई किराए (आने-जाने का कुल खर्च) या वास्तविक किराया, जो भी कम हो, की प्रतिपूर्ति. |
| 2. डिप्टी वाइस प्रेसिडेंट (DVP) – नागरिक-केंद्रित पहल | |
| 3. उप वाइस प्रेसिडेंट (DVP) – साइबर सुरक्षा | |

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 स्वतंत्र सत्यापन के आधार पर नियुक्ति/तैनाती से इनकार करने का अधिकार अपने पास सुरक्षित रखता है.**

**डिसक्लेमर (डिजिटल पर्सनल डेटा प्रोटेक्शन अधिनियम, 2023)**

xx. **इस पद के लिए आवेदन करके आप स्वेच्छा से, पूर्ण जानकारी के साथ तथा बिना किसी शर्त के, बैंक को अपनी व्यक्तिगत जानकारी (Personal Data) एकत्रित करने, उसका प्रसंस्करण (Processing) करने तथा भर्ती प्रक्रिया की आवश्यकता के अनुसार संबंधित डेटा प्रोसेसरों (Data Processors) के साथ साझा करने की अपनी सहमति प्रदान करते हैं. यह कार्य डिजिटल पर्सनल डेटा प्रोटेक्शन अधिनियम, 2023 तथा उसके अंतर्गत बनाए गए नियमों (सामूहिक रूप से ''अधिनियम'') के अनुरूप किया जाएगा. बैंक ने अपने पास उपलब्ध अथवा अपने नियंत्रणाधीन व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करने तथा किसी भी प्रकार के डेटा उल्लंघन (Data Breach) को रोकने के लिए सभी उचित सुरक्षा उपाय लागू किए हैं. आपकी व्यक्तिगत जानकारी को पूर्ण गोपनीयता के साथ संभाला जाएगा और इसका उपयोग केवल विज्ञापित पद के लिए आपकी पात्रता, योग्यता, प्रमाण-पत्रों तथा उम्मीदवारी के मूल्यांकन एवं सत्यापन हेतु किया जाएगा, साथ ही अधिनियम के अंतर्गत अनुमत अन्य वैध उद्देश्यों के लिए भी इसका उपयोग किया जा सकता है.**

किसी भी 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**
**07.08.2026**

**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/2026-27/11 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)