SBI

भारतीय स्टेट बैंक
केंद्रीय भर्ती एवं पदोन्नति विभाग,
कॉर्पोरेट केंद्र, मुंबई
फोन: 022-2282 0427, ईमेल: crpd@sbi.co.in

भारतीय स्टेट बैंक को ''ग्लोबल फाइनेंस'' द्वारा वर्ष 2024 के लिए ''भारत में सर्वश्रेष्ठ बैंक'' के रूप में मान्यता दी गई.

अनुबंध आधार पर विशेषज्ञ संवर्ग के अधिकारियों की नियुक्ति

विज्ञापन सं. CRPD/SCO/2025-26/08

आवेदन का ऑनलाइन पंजीकरण और शुल्क का भुगतान: दिनांक 25.08.2025 से 15.09.2025 तक

भारतीय स्टेट बैंक विशेषज्ञ संवर्ग के निम्नलिखित पद पर नियुक्ति के लिए भारतीय नागरिकों से ऑनलाइन आवेदन आमंत्रित करता है. उम्मीदवारों से अनुरोध है कि वे बैंक की वेबसाइट https://bank.sbi/careers/current-openings में दिए गए लिंक के माध्यम से ऑनलाइन आवेदन करें.

1. पंजीकरण की प्रक्रिया 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 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 हैं.**
3. **उम्मीदवार एक से अधिक पदों के लिए आवेदन कर सकते हैं.**
4. **एक से अधिक आवेदनों की स्थिति में, केवल अंतिम वैध (पूर्णत: भरा) आवेदन ही मान्य होगा, अन्य पंजीकरणों के लिए भुगतान किया गया आवेदन शुल्क/सूचना शुल्क जब्त कर लिया जाएगा.**
5. उम्मीदवारों को सभी आवश्यक दस्तावेज़ (संक्षिप्त बायोडाटा, पहचान का प्रमाण, आयु प्रमाण, जाति प्रमाण पत्र, पीडब्ल्यूबीडी प्रमाण पत्र (यदि लागू हो), शैक्षणिक योग्यता, अनुभव आदि) अपलोड करने की आवश्यकता है. ऐसा न करने पर उनके आवेदन/उम्मीदवारी पर शॉर्टलिस्टिंग/साक्षात्कार के लिए विचार नहीं किया जाएगा.
6. 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.
7. यदि उम्मीदवार को साक्षात्कार के लिए बुलाया जाता है और यदि वह पात्रता मानदंडों **(आयु, शैक्षणिक 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.
8. उम्मीदवारों को सूचित किया जाता है कि वे बैंक की वेबसाइट **https://bank.sbi/careers** को विवरणों एवं नई जानकारी (शॉर्टलिस्ट किए गए/चयनित उम्मीदवारों की सूची सहित) हेतु देखें. **कॉल (लेटर/सूचना), जहां आवश्यक हो, केवल ईमेल द्वारा भेजा जाएगा. (कागजी प्रति नहीं भेजी जाएगी).**
9. **सभी संशोधन/शुद्धि पत्र (यदि कोई है) केवल बैंक की वेबसाइट पर अपलोड किए जाएंगे.**
10. 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.
11. **इस कार्यालय को** आवेदन एवं अन्य दस्तावेज़ों की कागजी प्रतियाँ भेजने की आवश्यकता नहीं है.

क. पद/रिक्तियाँ/पदस्थापना का संभावित स्थान का विवरण:

क्र. सं.	पद का नाम	रिक्तियाँ		01.08.2025 को आयु (वर्षों में)#		पदस्थापना का संभावित स्थान++
		अनारक्षित	कुल	न्यूनतम	अधिकतम	
1	सेंटर हेड (सीएच)	1	1	45	50	मुंबई/नवी मुंबई
2	सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नीति एवं साइबर अकादमी	1	1	38	50	मुंबई/नवी मुंबई
3	सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर परामर्श	1	1	38	50	मुंबई/नवी मुंबई
4	सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नवाचार और अनुसंधान	1	1	38	50	मुंबई/नवी मुंबई
5	डिप्टी वाइस प्रेसिडेंट – साइबर नीति हब	1	1	35	45	मुंबई/नवी मुंबई
6	डिप्टी वाइस प्रेसिडेंट – साइबर अकादमी	1	1	35	45	मुंबई/नवी मुंबई
7	डिप्टी वाइस प्रेसिडेंट – साइबर नवाचार और अनुकरण लैब	1	1	35	45	मुंबई/नवी मुंबई
8	डिप्टी वाइस प्रेसिडेंट – साइबर बेंचमार्किंग हब	1	1	35	45	मुंबई/नवी मुंबई
9	डिप्टी वाइस प्रेसिडेंट – साइबर अनुसंधान	1	1	35	45	मुंबई/नवी मुंबई
10	डिप्टी वाइस प्रेसिडेंट – साइबर डिफेंस एवं इंटेलिजेंस	1	1	35	45	मुंबई/नवी मुंबई
11	डिप्टी वाइस प्रेसिडेंट – साइबर नागरिक केंद्रित पहल	1	1	35	45	मुंबई/नवी मुंबई
12	डिप्टी वाइस प्रेसिडेंट – साइबर परामर्श	1	1	35	45	मुंबई/नवी मुंबई

संक्षेपाक्षर: यूआर – अनारक्षित;

++ बैंक ऐसे संविदा पर नियुक्त अधिकारियों (OECs) की सेवाओं को भारत में भारतीय स्टेट बैंक के किसी भी कार्यालय में स्थानांतरित करने या अपने किसी सहयोगी/सहायक या किसी अन्य संगठन में सेवा की आवश्यकता के आधार पर प्रतिनियुक्त करने का अधिकार सुरक्षित रखता है. किसी विशिष्ट स्थान/कार्यालय में तैनाती/स्थानांतरण के अनुरोध पर विचार नहीं किया जा सकता है.

महत्वपूर्ण बिंदु:

i. ऊपर उल्लिखित आरक्षित रिक्त–पदों सहित रिक्तियों की संख्या **अनंतिम है** और यह बैंक की वास्तविक आवश्यकता के अनुसार **बदल सकती है.**

ii. विभिन्न पदों के लिए निर्धारित शैक्षणिक योग्यता न्यूनतम है. उम्मीदवार को **निर्दिष्ट तिथियों के अनुसार योग्यता** और **प्रासंगिक पूर्णकालिक अनुभव** होना चाहिए.

iii. निर्धारित दिव्यांग (पीडब्ल्यूबीडी) व्यक्ति, जिनके लिए कोई आरक्षण का उल्लेख नहीं किया गया है, सहित आरक्षित श्रेणी से संबंधित उम्मीदवार सामान्य श्रेणी के लिए घोषित रिक्तियों के लिए आवेदन करने के लिए स्वतंत्र हैं, बशर्ते वे सामान्य श्रेणी के लिए लागू सभी पात्रता मानदंडों को पूरा करते हों.

iv. विभिन्न श्रेणियों के तहत आरक्षण (यदि लागू हो) प्रचलित सरकारी दिशानिर्देशों के अनुसार होगा.

v. नियोक्ता से संबंधित अनुभव प्रमाण पत्र में विशेष रूप से उल्लेख होना चाहिए कि उम्मीदवार को संबंधित क्षेत्र में अपेक्षित अनुभव है. **उचित अनुभव प्रमाण पत्र प्रस्तुत न करने पर बैंक को किसी भी समय उम्मीदवारी रद्द करने का अधिकार है.**

vi. बैंक किसी भी स्तर पर इस भर्ती प्रक्रिया को पूरी तरह से या किसी विशेष पद के लिए रद्द करने का अधिकार सुरक्षित रखता है.

vii. केवल बेंचमार्क दिव्यांगता वाले व्यक्ति ही बेंचमार्क दिव्यांगता (PwBD) श्रेणी के तहत आरक्षण के लिए पात्र होंगे. **'निर्धारित अशक्तता वाले व्यक्ति'** से आशय उस व्यक्ति से है जो विनिर्दिष्ट अशक्तता का कम से कम 40 प्रतिशत अश**क्त** हो, उन मामलों में जहाँ विनिर्दिष्ट अशक्तता को मापन श्रेणी में नहीं रखा गया है. प्रमाणित करने वाले प्राधिकारी के प्रमाणन के अनुसार इसके अंतर्गत वह अशक्त व्यक्ति भी आता है जिसकी अशक्तता को मापन श्रेणी में रखा गया है. दिव्यांगजन (पीडब्ल्यूबीडी) के लिए आरक्षित बैकलॉग रिक्तियों को संबंधित श्रेणी में संदर्भित दिव्यांगता (पीडब्ल्यूबीडी) वाले उम्मीदवारों द्वारा भरा जाएगा. यदि उस श्रेणी से कोई उपयुक्त उम्मीदवार उपलब्ध नहीं है, तो ऐसे बैकलॉग को अन्य पात्र दिव्यांगजन उम्मीदवारों के बीच परस्पर अदला–बदली द्वारा भरा जाएगा, बशर्ते कि पद ऐसी निशक्तताओं के लिए उपयुक्त निर्धारित किए गए हों.

viii. **स्थानांतरण नीति:** बैंक संविदा पर नियोजित ऐसे अधिकारियों की सेवाओं को सेवा की अनिवार्यता के आधार पर भारत में भारतीय स्टेट बैंक के किसी भी कार्यालय में स्थानांतरित करने या अपने किसी सहयोगी/सहायक या किसी अन्य संगठन में प्रतिनियुक्त करने का अधिकार सुरक्षित रखता है. **किसी विशिष्ट स्थान/कार्यालय में तैनाती/स्थानांतरण के किसी भी अनुरोध पर विचार नहीं किया जा सकता है.**

ix. **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 में उनकी आयु के आधार पर अवरोही क्रम में रैंक प्रदान की जाएगी.

x. 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 बाद 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 पत्राचार पर विचार नहीं किया जाएगा.**

xi. **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 नियुक्ति प्रस्ताव पत्र जारी करने की तारीख तक उनके बकाया को नियमित/चुकाया नहीं है, वे पद पर नियुक्ति के लिए पात्र नहीं होंगे. हालांकि, ऐसे उम्मीदवार जिन्होंने 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 नियुक्ति के लिए पात्र नहीं हैं. **उम्मीदवारों को सलाह दी जाती है कि वे आवेदन करने से पहले सिबिल (CIBIL) स्कोर/स्थिति की जांच/पुष्टि कर लें.**

xii. **जो उम्मीदवार सरकार/अर्ध-सरकारी कार्यालयों, राष्ट्रीयकृत बैंकों और वित्तीय संस्थानों सहित सार्वजनिक क्षेत्र के प्रतिष्ठानों और एसबीआई समूह की कंपनियों 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.**

ख. पारिश्रमिक और अनुबंध अवधि:

क्र.सं.	पद नाम	वार्षिक सीटीसी की ऊपरी सीमा^ (लाख रु. में)	वार्षिक सीटीसी के विभिन्न मद	संविदा अवधि $
1	सेंटर हेड (सीएच) (क्रम संख्या 1)	**100.00**	नियत वेतन: सीटीसी का 90% परिवर्ती वेतन: सीटीसी का 10% वार्षिक वेतन वृद्धि बैंड: 7% से 10%	**3 वर्ष** परस्पर सहमत निबंधनों और शर्तों पर बैंक के विवेकानुसार 2 वर्ष की अतिरिक्त अवधि के लिए नवीनीकृत किया जा सकता है. (कुल नियुक्ति अवधि 5 वर्ष से अधिक नहीं होनी चाहिए.)
2	सीनियर वाइस प्रेसिडेंट (एसवीपी) (सभी तीन पदों के लिए- क्रम संख्या 2 से 4)	**80.00**		
3	डिप्टी वाइस प्रेसिडेंट (सभी आठ पदों के लिए- क्रम संख्या 5 से 12)	**60.00**		

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

$ संविदा अवधि 3 वर्ष है. संविदा को किसी भी समय, बिना किसी पूर्वाग्रह के, किसी भी पक्ष की ओर से 90 दिन का नोटिस देकर या उसके बदले में 90 दिन की वेतन राशि का भुगतान/सरेंडर करने पर समाप्त किया जा सकता है.

****दूसरे वर्ष से 7-10% (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 नीचे	शून्य

अन्य सुविधाएं: देय नहीं

ग. आवश्यक शैक्षणिक योग्यता/योग्यता के बाद का अनुभव/विशिष्ट कौशल आदि का विवरण.

पद संख्या	पद	अन्य अनिवार्य/अधिमान्य योग्यता/प्रमाणन (01.08.2025 तक)	योग्यता-पश्चात् कार्य अनुभव (01.08.2025 तक)	अपेक्षित विशिष्ट कौशल:
$ टिप्पणी: प्रशिक्षण एवं शिक्षण अनुभव को पात्रता के लिए नहीं गिना जाएगा.				
1	सेंटर हेड (सीएच)	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** ● आईटी/ साइबर/ आईटी सुरक्षा नवाचार/ साइबर अनुसंधान/ साइबर उद्योग अनुसंधान/ आईटी परियोजना प्रबंधन में कम से कम 8-10 वर्षों के अनुभव के साथ 20+ वर्षों का समग्र अनुभव, साथ ही सीओई (उत्कृष्टता केंद्र) में काम करने या उसकी स्थापना करने का अनुभव. **अधिमान्य:** ● बैंकिंग और वित्तीय उद्योग के नियमों और अनुपालन अपेक्षाओं की ठोस समझ. इसमें प्रमुख नियमों का सिद्ध ज्ञान और बीएफएसआई आईटी/ सुरक्षा अनुभव शामिल है, जिसमें आरबीआई का साइबर सुरक्षा ढांचा, सेबी के साइबर सुरक्षा दिशानिर्देश, डेटा सुरक्षा कानून/ पीसीआई-डीएसएस/ एनआईएसटी ढांचा, और बीएफएसआई संदर्भ में विनियामक अनुपालन शामिल हैं, लेकिन इन्हीं तक सीमित नहीं. आवेदन के दौरान दस्तावेज़ जमा करना अनिवार्य नहीं होगा. हालाँकि, यदि बायोडाटा/ आवेदन में उल्लेख किया गया है, तो साक्षात्कार के समय उसका सत्यापन किया जाएगा. ● सुरक्षा प्रोफेशनलों को प्रेरित और विकसित करने की क्षमता के साथ उत्कृष्ट नेतृत्व और टीम प्रबंधन कौशल. ● दबाव में भी ठोस निर्णय लेने की क्षमता के साथ, मज़बूत विश्लेषणात्मक और समस्या-समाधान क्षमताएँ. ● तकनीकी और गैर-तकनीकी हितधारकों को जटिल सुरक्षा अवधारणाओं से अवगत कराने के लिए मौखिक और लिखित दोनों तरह के प्रभावी संप्रेषण कौशल.	● सेंटर हेड को साइबर सुरक्षा उत्कृष्टता केंद्र के संचालन को समग्र रूप से संचालित करने के लिए सशक्त नेतृत्व, रणनीतिक सोच, संचार और तकनीकी विशेषज्ञता सहित विविध कौशलों की आवश्यकता होती है. ● उसे संसाधनों का प्रभावी प्रबंध करना, टीमों का नेतृत्व करनाऔर यह सुनिश्चित करना होगा कि अनुसंधान परियोजनाएँ संगठनात्मक लक्ष्यों के अनुरूप हों. प्रमुख कौशलों में परियोजना नियोजन, आलोचनात्मक सोच, डेटा प्रबंधन, नेतृत्व गुण और नैतिक जागरूकता शामिल हैं, लेकिन इन्हीं तक सीमित नहीं. ● कार्यक्रम प्रबंधन सिद्धांतों और प्रक्रियाओं का ज्ञान, मज़बूत पारस्परिक कौशल, लोगों का प्रबंधन और मार्गदर्शन कौशल, छोटी टीमों में काम करने और स्वतंत्र रूप से परियोजनाओं का प्रबंधन करने की क्षमता. ● उत्कृष्ट मौखिक और लिखित संप्रेषण. ● मज़बूत नैतिक दिशानिर्देश जो सार्वजनिक सेवा, नैतिकता और सत्यनिष्ठा के संगठनात्मक मूल्यों को बनाए रखेंगे. ● ग्राहक और नागरिक केंद्रित नवीन प्रथाओं का कार्यान्वयन. सरकार, शिक्षा और उद्योग में सीनियर-स्तरीय हितधारकों के साथ बातचीत और प्रबंधन करने की क्षमता. ● एसबीआई के उद्देश्यों के साथ तालमेल बिठाना और काम करना तथा इसकी साइबर सुरक्षा स्थिति को बेहतर बनाना. ● साइबर सुरक्षा नीति और व्यवहार में अनुभव, एक नवाचार केंद्रित कार्यक्रम को शुरू से अंत तक चलाने का ज्ञान और अनुभव. ● साइबर सुरक्षा तकनीक की समझ और अनुभव तथा उद्देश्यपूर्ण निष्पादन के लिए सुरक्षा अनुसंधानकर्ताओं की टीम का नेतृत्व करने की क्षमता. ● उन्नत साइबर सुरक्षा अवधारणाओं और नवीनतम तकनीकी प्रगतियों और व्यवधानों की समझ.

2	सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नीति एवं साइबर अकादमी	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर नीति और साइबर सुरक्षा में सीनियर स्तर पर कम से कम 8-10 वर्षों के अनुभव सहित कुल मिलाकर 15+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर सुरक्षा से संबंधित परामर्श वातावरण में कार्य करने या उसका प्रबंधन करने का अनुभव एक अतिरिक्त लाभ है. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना करने या उसमें सीनियर स्तर पर कार्य करने का अनुभव. • बैंकिंग और वित्तीय उद्योग के नियमों और अनुपालन अपेक्षाओं की ठोस समझ. इसमें प्रमुख नियमों का सिद्ध ज्ञान और बीएफएसआई आईटी/ सुरक्षा अनुभव शामिल है, जिसमें आरबीआई का साइबर सुरक्षा ढांचा, सेबी के साइबर सुरक्षा दिशानिर्देश, डेटा सुरक्षा कानून/ पीसीआई–डीएसएस/ एनआईएसटी ढांचा, और बीएफएसआई संदर्भ में विनियामक अनुपालन शामिल हैं, लेकिन इन्हीं तक सीमित नहीं. आवेदन के दौरान दस्तावेज़ जमा करना अनिवार्य नहीं होगा. हालाँकि, यदि बायोडाटा/ आवेदन में उल्लेख किया गया है, तो साक्षात्कार के समय उसका सत्यापन किया जाएगा.	• एसवीपी– साइबर नीति एवं साइबर अकादमी को विविध कौशलों की आवश्यकता होती है, जिनमें मज़बूत नेतृत्व, रणनीतिक सोच, संप्रेषण और तकनीकी विशेषज्ञता शामिल है. • उसे संसाधनों का प्रभावी प्रबंध करना, टीमों का नेतृत्व करनाऔर यह सुनिश्चित करना होगा कि अनुसंधान परियोजनाएँ संगठनात्मक लक्ष्यों के अनुरूप हों. • साइबर संबंधी नीति के वितरण प्रबंधन से संबंधित तकनीकी और प्रबंधकीय कौशल. • परियोजना नियोजन, आलोचनात्मक सोच, डेटा प्रबंधन, नेतृत्व गुण और नैतिक जागरूकता. • कार्यक्रम प्रबंधन सिद्धांतों और प्रक्रियाओं का ज्ञान, मज़बूत पारस्परिक कौशल, लोगों का प्रबंधन और मार्गदर्शन कौशल, छोटी टीमों में काम करने और स्वतंत्र रूप से परियोजनाओं का प्रबंधन करने की क्षमता. • उत्कृष्ट मौखिक और लिखित संप्रेषण. • मज़बूत नैतिक दिशानिर्देश जो सार्वजनिक सेवा, नैतिकता और सत्यनिष्ठा के संगठनात्मक मूल्यों को बनाए रखेंगे. • एसबीआई के उद्देश्यों के साथ तालमेल बिठाना और काम करना तथा इसकी साइबर सुरक्षा स्थिति को बेहतर बनाना. • साइबर सुरक्षा नीति और व्यवहार में अनुभव, एक नवाचार केंद्रित कार्यक्रम को शुरू से अंत तक चलाने का ज्ञान और अनुभव. • उन्नत साइबर सुरक्षा अवधारणाओं और नवीनतम तकनीकी प्रगतियों और व्यवधानों की समझ. • साइबर सुरक्षा खतरों, प्रौद्योगिकियों और उद्योग के रुझानों की समझ. • उत्कृष्ट नेतृत्व, संप्रेषण और पारस्परिक कौशल. • तेज़–तर्रार वातावरण में रणनीतिक रूप से सोचने और नवाचार को आगे बढ़ाने की क्षमता.
3	सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर परामर्श	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर नीति और साइबर सुरक्षा में सीनियर स्तर पर कम से कम 8-10 वर्षों के अनुभव सहित कुल मिलाकर 15+ वर्षों का समग्र अनुभव. साइबर सुरक्षा संबंधी परामर्श वातावरण में कार्य करने या उसका प्रबंधन करने का अनुभव आवश्यक है. **अधिमान्य:** • साइबर सुरक्षा से संबंधित परामर्श वातावरण में काम करने या उसका प्रबंधन करने का अनुभव. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना करने या उसमें सीनियर स्तर पर काम करने का अनुभव एक अतिरिक्त लाभ है. • बैंकिंग और वित्तीय उद्योग के नियमों और अनुपालन अपेक्षाओं की ठोस समझ. इसमें प्रमुख नियमों का सिद्ध ज्ञान और बीएफएसआई आईटी/ सुरक्षा अनुभव शामिल है, जिसमें आरबीआई का साइबर सुरक्षा ढांचा, सेबी के साइबर सुरक्षा दिशानिर्देश, डेटा सुरक्षा कानून/ पीसीआई–डीएसएस/ एनआईएसटी ढांचा, और बीएफएसआई संदर्भ में विनियामक अनुपालन शामिल हैं, लेकिन इन्हीं तक सीमित नहीं. आवेदन के दौरान दस्तावेज़ जमा करना अनिवार्य नहीं होगा. हालाँकि, यदि बायोडाटा/ आवेदन में उल्लेख किया गया है, तो साक्षात्कार के समय उसका सत्यापन किया जाएगा.	• सीनियर वाइस प्रेसिडेंट, साइबर परामर्श को सशक्त नेतृत्व, रणनीतिक सोच, संप्रेषण और तकनीकी विशेषज्ञता सहित विविध कौशल की आवश्यकता होती है. • विभिन्न हितधारकों के साथ परिणाम–उन्मुख रणनीतिक सलाहकार भूमिकाएँ निभाने की क्षमता और अनुभव. • ग्राहक जागरूकता कार्यक्रमों का रणनीतिक विकास और कार्यान्वयन • साइबर सुरक्षा कार्यक्रम की प्रभावशीलता का मूल्यांकन और संचालन करने का कौशल • शैक्षणिक संस्थानों, उद्योग भागीदारों और सरकारी एजेंसियों के साथ सहयोग का अनुभव अत्यधिक वांछनीय है. • उसे संसाधनों का प्रभावी प्रबंध करना, टीमों का नेतृत्व करनाऔर यह सुनिश्चित करना होगा कि अनुसंधान परियोजनाएँ संगठनात्मक लक्ष्यों के अनुरूप हों. • परियोजना नियोजन, आलोचनात्मक सोच, डेटा प्रबंधन, नेतृत्व गुण और नैतिक जागरूकता. • कार्यक्रम प्रबंधन सिद्धांतों और प्रक्रियाओं का ज्ञान, मज़बूत पारस्परिक कौशल, लोगों का प्रबंधन और मार्गदर्शन कौशल, छोटी टीमों में काम करने और स्वतंत्र रूप से परियोजनाओं का प्रबंधन करने की क्षमता. • उत्कृष्ट मौखिक और लिखित संप्रेषण. • मज़बूत नैतिक दिशानिर्देश जो सार्वजनिक सेवा, नैतिकता और सत्यनिष्ठा के संगठनात्मक मूल्यों को बनाए रखेंगे. • एसबीआई के उद्देश्यों के साथ तालमेल बिठाना और काम करना तथा इसकी साइबर सुरक्षा स्थिति को बेहतर बनाना. • साइबर सुरक्षा तकनीक की समझ और अनुभव तथा उद्देश्यपूर्ण निष्पादन के लिए सुरक्षा अनुसंधानकर्ताओं की टीम का नेतृत्व करने की क्षमता. • उन्नत साइबर सुरक्षा प्रवृत्तियों, ख़तरा विश्लेषण, बाज़ार समझ और महत्वपूर्ण विश्लेषण क्षमताओं की समझ. • जन–आधारित कार्यक्रमों के लिए साइबर सुरक्षा पहलों का नेतृत्व करने, उनकी प्रभावशीलता और उनमें सुधार का आकलन करने का सिद्ध अनुभव. • साइबर सुरक्षा खतरों, प्रौद्योगिकियों और उद्योग प्रवृत्तियों की गहरी समझ. • उत्कृष्ट नेतृत्व, संप्रेषण और पारस्परिक कौशल.

4	**सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नवाचार और अनुसंधान**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • नवाचार/प्रासंगिक अनुसंधान एवं विकास में कम से कम 8-10 वर्षों के अनुभव के साथ 15+ वर्षों का समग्र अनुभव. **अधिमान्य:** • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना करने या उसमें सीनियर स्तर पर काम करने का अनुभव एक अतिरिक्त लाभ है. • बैंकिंग और वित्तीय उद्योग के नियमों और अनुपालन अपेक्षाओं की ठोस समझ. इसमें प्रमुख नियमों का सिद्ध ज्ञान और बीएफएसआई आईटी/ सुरक्षा अनुभव शामिल है, जिसमें आरबीआई का साइबर सुरक्षा ढांचा, सेबी के साइबर सुरक्षा दिशानिर्देश, डेटा सुरक्षा कानून/ पीसीआई-डीएसएस/ एनआईएसटी ढांचा, और बीएफएसआई संदर्भ में विनियामक अनुपालन शामिल हैं, लेकिन इन्हीं तक सीमित नहीं. आवेदन के दौरान दस्तावेज़ जमा करना अनिवार्य नहीं होगा. हालाँकि, यदि बायोडाटा/ आवेदन में उल्लेख किया गया है, तो साक्षात्कार के समय उसका सत्यापन किया जाएगा.	• सीनियर एसवीपी, नवाचार एवं अनुसंधान को मज़बूत नेतृत्व, रणनीतिक सोच, संचार और तकनीकी विशेषज्ञता सहित विविध कौशलों की आवश्यकता होती है. • उन्हें संसाधनों का प्रभावी प्रबंधन, टीमों का नेतृत्व और यह सुनिश्चित करना होगा कि अनुसंधान परियोजनाएँ संगठनात्मक लक्ष्यों के अनुरूप हों. • नवाचार और अनुसंधान प्रयोगशालाओं की स्थापना और रखरखाव. • अनुसंधान परियोजनाओं को आगे बढ़ाने और अनुसंधान करते समय परिणाम-उन्मुख दृष्टिकोण अपनाने का अनुभव. • परियोजना नियोजन, आलोचनात्मक सोच, डेटा प्रबंधन, नेतृत्व गुण और नैतिक जागरूकता. • कार्यक्रम प्रबंधन सिद्धांतों और प्रक्रियाओं का ज्ञान, मज़बूत पारस्परिक कौशल, लोगों का प्रबंधन और मार्गदर्शन कौशल, छोटी टीमों में काम करने और स्वतंत्र रूप से परियोजनाओं का प्रबंधन करने की क्षमता. • उत्कृष्ट मौखिक और लिखित संप्रेषण • मज़बूत नैतिक दिशानिर्देश जो सार्वजनिक सेवा, नैतिकता और सत्यनिष्ठा के संगठनात्मक मूल्यों को बनाए रखेंगे. • एसबीआई के उद्देश्यों के साथ तालमेल बिठाना और काम करना तथा उसकी साइबर सुरक्षा स्थिति को बेहतर बनाना. • साइबर सुरक्षा नीति और व्यवहार में अनुभव, नवाचार-केंद्रित कार्यक्रम को शुरू से अंत तक चलाने का ज्ञान और अनुभव. • साइबर सुरक्षा तकनीक की समझ और अनुभव तथा उद्देश्यपूर्ण परिणाम प्राप्त करने के लिए सुरक्षा अनुसंधानकर्ताओं की टीम का नेतृत्व करने की क्षमता. • उन्नत साइबर सुरक्षा अवधारणाओं और नवीनतम तकनीकी प्रगतियों और व्यवधानों की समझ. • साइबर सुरक्षा अनुसंधान और नवाचार टीमों का नेतृत्व करने का सिद्ध अनुभव, और प्रभावशाली समाधान प्रदान करने का एक मज़बूत ट्रैक रिकॉर्ड. • साइबर सुरक्षा खतरों, तकनीकों और उद्योग की प्रवृत्तियों की गहरी समझ. • उत्कृष्ट नेतृत्व, संप्रेषण और पारस्परिक कौशल. • तेज़-तर्रार वातावरण में रणनीतिक रूप से सोचने और नवाचार को आगे बढ़ाने की क्षमता. • शैक्षणिक संस्थानों, उद्योग भागीदारों और सरकारी एजेंसियों के साथ सहयोग का अनुभव अत्यधिक वांछनीय है.
5	**डिप्टी वाइस प्रेसिडेंट – साइबर नीति हब**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर नीति में कम से कम 8-10 वर्षों के अनुभव के साथ 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर सुरक्षा से संबंधित नीति/ अभिशासन परिवेश में कार्य करने या उसका प्रबंधन करने का अनुभव एक अतिरिक्त लाभ है. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव एक अतिरिक्त लाभ है.	• साइबर सुरक्षा नीति हब प्रमुख के लिए विविध कौशल आवश्यक हैं, जिनमें तकनीकी विशेषज्ञता और नेतृत्व क्षमताएँ दोनों शामिल हों. • साइबर सुरक्षा नीति और व्यवहार में अनुभव, नवाचार-केंद्रित कार्यक्रमों को शुरू से अंत तक चलाने का ज्ञान और अनुभव. • व्यावसायिक उद्देश्यों के अनुरूप दीर्घकालिक साइबर सुरक्षा नीतियाँ बनाने की क्षमता. • नीति की वकालत और प्रसार क्षेत्रों में अनुभव. • साइबर नीतियों के लिए मेट्रिक्स बनाना, उनकी समीक्षा करना और उनका प्रबंधन करना. • आलोचनात्मक सोच, डेटा प्रबंधन, नेतृत्व गुण और नैतिक जागरूकता. • कार्यक्रम प्रबंधन सिद्धांतों और प्रक्रियाओं का ज्ञान, मज़बूत पारस्परिक कौशल, लोगों का प्रबंधन और मार्गदर्शन कौशल, छोटी टीमों में काम करने और स्वतंत्र रूप से परियोजनाओं का प्रबंधन करने की क्षमता. • उत्कृष्ट मौखिक और लिखित संप्रेषण • उन्नत साइबर सुरक्षा अवधारणाओं और नवीनतम तकनीकी प्रगति और व्यवधानों की समझ. • विनियामक परिवेशों का ज्ञान (विशेषकर साइबर सुरक्षा, आईटी और नवाचार में). • निरंतर विकसित हो रहे साइबर सुरक्षा परिदृश्य में नवीनतम खतरों, तकनीकों और सर्वोत्तम प्रथाओं से अपडेट रहना.

6	**डिप्टी वाइस प्रेसिडेंट – साइबर अकादमी**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर अकादमी और ज्ञान प्रसार भूमिकाओं में कम से कम 8-10 वर्षों के अनुभव सहित 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर सुरक्षा से संबंधित साइबर सुरक्षा प्रशिक्षणों में कार्य करने या उनका प्रबंधन करने का अनुभव. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	• मज़बूत नेतृत्व और प्रबंधन कौशल, साथ ही टीम को प्रेरित और प्रोत्साहित करने की क्षमता. • साइबर सुरक्षा क्षेत्रों का अच्छा तकनीकी ज्ञान. • तकनीकी कौशल का प्रशिक्षण और प्रसार, ज़रूरतों की पहचान और कौशल विकास एवं संवेदीकरण कार्यक्रमों का संचालन. • साइबर लैब और आधुनिक शिक्षण तकनीकों का ज्ञान. • उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल, साथ ही विविध श्रोताओं को जटिल तकनीकी अवधारणाओं को समझाने की क्षमता. • मज़बूत परियोजना प्रबंधन कौशल, साथ ही जटिल प्रशिक्षण पहलों की योजना बनाने, उन्हें व्यवस्थित करने और क्रियान्वित करने की क्षमता. • साइबर सुरक्षा प्रशिक्षण और शिक्षा से संबंधित जटिल समस्याओं की पहचान और समाधान करने की क्षमता। बदलती तकनीकों और उद्योग के रुझानों के साथ तालमेल बिठाने की क्षमता. • सार्वजनिक–निजी भागीदारी मॉडल या उत्कृष्टता केंद्र का अनुभव. • बीएफएसआई क्षेत्रीय साइबर सुरक्षा और जोखिमों की गहरी समझ.
7	**डिप्टी वाइस प्रेसिडेंट – साइबर नवाचार और अनुकरण लैब**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर नवाचार और अनुकरण में कम से कम 8-10 वर्षों के अनुभव के साथ 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर सुरक्षा नवाचार पहल और साइबर समाधानों के अनुकरण पर काम करने या प्रबंधन करने का अनुभव. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	• भविष्य की साइबर सुरक्षा तकनीकों, उभरते रुझानों और विघटनकारी तकनीकों में विभिन्न साइबर सुरक्षा क्षेत्रों की गहरी समझ. • विचार–मंथन, प्रोटोटाइपिंग और उत्पाद विकास सहित नवाचार पहलों का नेतृत्व करने या उनका समर्थन करने का सिद्ध अनुभव. • साइबर सुरक्षा से संबंधित क्लाउड कंप्यूटिंग, नेटवर्किंग और प्रोग्रामिंग भाषाओं जैसे क्षेत्रों में अनुभव के साथ मज़बूत तकनीकी पृष्ठभूमि. विविध टीमों और हितधारकों के साथ प्रभावी ढंग से सहयोग करने के लिए उत्कृष्ट नेतृत्व, संचार और पारस्परिक कौशल. • रणनीतिक रूप से सोचने और नवाचार प्रयासों को संगठन के व्यावसायिक उद्देश्यों के साथ संरेखित करने की क्षमता. जटिल साइबर सुरक्षा चुनौतियों की पहचान करने और उनका समाधान करने के लिए मज़बूत विश्लेषणात्मक और समस्या–समाधान कौशल. • बदलती व्यावसायिक आवश्यकताओं और उभरते खतरों के अनुकूल ढलने की क्षमता, नई चुनौतियों का सामना करने में लचीलापन और चपलता प्रदर्शित करना. • शैक्षणिक संस्थानों, उद्योग भागीदारों और सरकारी एजेंसियों के साथ सहयोग का अनुभव अत्यधिक वांछनीय है.
8	**डिप्टी वाइस प्रेसिडेंट – साइबर बेंचमार्किंग हब**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर सुरक्षा से संबंधित प्रक्रियाओं और तकनीकों के साइबर विश्लेषण/ बेंचमार्किंग में कम से कम 8-10 वर्षों के अनुभव सहित 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर समाधानों की रेटिंग/ ग्रेडिंग के साथ–साथ तकनीक और उत्पादों के साइबर सुरक्षा–संबंधी विश्लेषण में कार्य करने या प्रबंध करने का अनुभव. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	• उपयुक्त मेट्रिक्स और कार्यप्रणाली के चयन सहित साइबर सुरक्षा बेंचमार्किंग कार्यक्रमों को विकसित और कार्यान्वित करने का अनुभव. • निरंतर सुधार और सर्वोत्तम प्रथाओं के प्रति उत्कृष्टता केंद्र (सीओई) की प्रतिबद्धता का प्रदर्शन. • विभिन्न साइबर सुरक्षा क्षेत्रों की गहरी समझ, जिसमें ख़तरा खुफिया जानकारी, घटना प्रतिक्रिया, सुरक्षा संरचना और जोखिम प्रबंधन शामिल हैं. • विचार, प्रोटोटाइप और उत्पाद विकास सहित नवाचार पहलों का नेतृत्व या समर्थन करने का सिद्ध अनुभव. • क्लाउड कंप्यूटिंग, नेटवर्किंग और साइबर सुरक्षा से संबंधित प्रोग्रामिंग भाषाओं जैसे क्षेत्रों में अनुभव के साथ मज़बूत तकनीकी पृष्ठभूमि. विविध टीमों और हितधारकों के साथ प्रभावी ढंग से सहयोग करने के लिए उत्कृष्ट नेतृत्व, संप्रेषण और पारस्परिक कौशल. • जटिल साइबर सुरक्षा चुनौतियों की पहचान करने और उनका समाधान करने के लिए मज़बूत विश्लेषणात्मक और समस्या–समाधान कौशल. • बदलती व्यावसायिक आवश्यकताओं और उभरते खतरों के अनुकूल ढलने की क्षमता, नई चुनौतियों का सामना करने में लचीलापन और चपलता प्रदर्शित करना.

9	**डिप्टी वाइस प्रेसिडेंट – साइबर अनुसंधान**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर अनुसंधान में कम से कम 8-10 वर्षों के अनुभव सहित 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** • साइबर सुरक्षा अनुसंधान परियोजनाओं पर कार्य करने का अनुभव. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	• साइबर सुरक्षा सिद्धांतों, तकनीकों और सर्वोत्तम प्रथाओं की गहरी समझ. • अनुसंधान और विचार नेतृत्व पहलों का नेतृत्व करने का सिद्ध अनुभव. • मज़बूत विश्लेषणात्मक और समस्या–समाधान कौशल. • उत्कृष्ट संचार और प्रस्तुति कौशल. • साइबर सुरक्षा रणनीतियों को विकसित करने और लागू करने का अनुभव. • प्रासंगिक उद्योग मानकों और विनियमों का ज्ञान. • टीम के सदस्यों को सलाह देने और मार्गदर्शन करने का अनुभव. • यह भूमिका संगठन और व्यापक समुदाय के भीतर उच्च स्तर की साइबर सुरक्षा विशेषज्ञता का निर्माण और उसे बनाए रखने में मदद करती है. • साइबर सुरक्षा मानकों और सर्वोत्तम प्रथाओं के विकास में योगदान देकर, यह भूमिका साइबर सुरक्षा के भविष्य को आकार देने में मदद करती है. • क्लाउड कंप्यूटिंग, नेटवर्किंग और साइबर सुरक्षा से संबंधित प्रोग्रामिंग भाषाओं जैसे क्षेत्रों में अनुभव के साथ मज़बूत तकनीकी पृष्ठभूमि। विविध टीमों और हितधारकों के साथ प्रभावी ढंग से सहयोग करने के लिए उत्कृष्ट नेतृत्व, संप्रेषण और पारस्परिक कौशल. • जटिल साइबर सुरक्षा चुनौतियों की पहचान करने और उनका समाधान करने के लिए मज़बूत विश्लेषणात्मक और समस्या–समाधान कौशल.
10	**डिप्टी वाइस प्रेसिडेंट – साइबर डिफेंस एवं इंटेलिजेंस**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** • साइबर डिफेंस एवं इंटेलिजेंस क्षेत्र में कम से कम 8-10 वर्षों के अनुभव सहित कुल मिलाकर 12+ वर्षों का अनुभव. **अधिमान्य:** • फोरेंसिक, मैलवेयर विश्लेषण, थ्रेट हंटिंग, घटना प्रतिक्रिया और थ्रेट इंटेलिजेंस एकीकरण/निर्माण से संबंधित साइबर सुरक्षा उपकरण पर काम करने या उसे प्रबंधित करने का अनुभव. • आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. • किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	• साइबर सुरक्षा जोखिमों, घटनाओं और शमन योजनाओं के संबंध में सीनियर प्रबंधन, व्यावसायिक इकाइयों और अन्य हितधारकों के साथ प्रभावी ढंग से संवाद करना. • साइबर सुरक्षा सिद्धांतों और सर्वोत्तम प्रथाओं की गहरी समझ. • फायरवॉल, घुसपैठ का पता लगाने/रोकथाम प्रणाली, SIEM और एंडपॉइंट सुरक्षा सहित सुरक्षा तकनीकों में विशेषज्ञता. • ख़तरा इंटेलिजेंस प्लेटफ़ॉर्म और उपकरणों में दक्षता. • साइबर फोरेंसिक और घटना प्रतिक्रिया प्रक्रियाओं का ज्ञान. • साइबर सुरक्षा तकनीकों और प्रथाओं में मज़बूत तकनीकी पृष्ठभूमि. • उत्कृष्ट संचार, पारस्परिक और नेतृत्व कौशल • इस संभावना का विश्लेषण करना कि कोई उभरता हुआ ख़तरा उनके संगठन को प्रभावित करेगा और कमज़ोरियों की पहचान करना. • शमन और सुधार प्रयासों की प्रभावशीलता को सक्षम करने के लिए व्यवसाय के लिए रिपोर्ट और सिफ़ारिशें परिभाषित करना. • साइबर सुरक्षा सिद्धांतों, तकनीकों और सर्वोत्तम प्रथाओं की अच्छी समझ. • साइबर सुरक्षा पेशेवरों की एक टीम का नेतृत्व, मार्गदर्शन और विकास करने की क्षमता. • एक व्यापक साइबर सुरक्षा रणनीति विकसित करने और उसे लागू करने की क्षमता. • सभी स्तरों पर हितधारकों के साथ प्रभावी ढंग से संवाद करने के लिए उत्कृष्ट लिखित और मौखिक संप्रेषण कौशल. • जटिल सुरक्षा मुद्दों का विश्लेषण करने और प्रभावी समाधान विकसित करने की क्षमता. • साइबर सुरक्षा जोखिमों का आकलन, शमन और प्रबंधन करने की क्षमता. • साइबर सुरक्षा घटनाओं के प्रबंधन और प्रतिक्रिया का अनुभव. • प्रासंगिक साइबर सुरक्षा मानकों, विनियमों और सर्वोत्तम प्रथाओं का ज्ञान.

11	**डिप्टी वाइस प्रेसिडेंट – साइबर नागरिक केंद्रित पहल**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** ● साइबर नागरिक केंद्रित क्षेत्र में कम से कम 8-10 वर्षों के अनुभव सहित 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** ● विभिन्न माध्यमों/ विधियों के माध्यम से साइबर सुरक्षा से संबंधित नागरिक जागरूकता गतिविधि जैसे साइबर से संबंधित जन और विशिष्ट जागरूकता कार्यक्रमों में कार्य करने या उनका प्रबंधन करने का अनुभव. ● आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. ● किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	● मज़बूत नेतृत्व और प्रबंधन कौशल. ● नागरिक और अंतिम उपयोगकर्ता सुरक्षा कार्यक्रमों का संचालन और स्वामित्व तथा उनकी प्रभावशीलता का आकलन. ● आउटरीच और साइबर उपयोगकर्ता सुरक्षा के लिए मेट्रिक्स बनाना और कार्यक्रम के विकास पर नज़र रखना. ● उत्कृष्ट संप्रेषण और अंतर्वैयक्तिक कौशल. ● आईटी, साइबर सुरक्षा और डेटा प्रबंधन जैसे प्रासंगिक क्षेत्रों में तकनीकी विशेषज्ञता. ● परियोजना प्रबंधन और कार्यक्रम कार्यान्वयन का अनुभव. ● प्रासंगिक नीतियों, विनियमों और सर्वोत्तम प्रथाओं का ज्ञान. ● तेज़–तर्रार वातावरण में प्रभावी ढंग से काम करने की क्षमता. ● हितधारक जुड़ाव और संबंध प्रबंधन का अनुभव. ● गरिक–केंद्रित पहलों में शामिल प्रोफ़ेशनलों की टीम को सलाह देना.
12	**डिप्टी वाइस प्रेसिडेंट – साइबर परामर्श**	**अनिवार्य:** बुनियादी योग्यताएँ: भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में बीई/ बीटेक डिग्री. **या** भारत सरकार द्वारा मान्यता प्राप्त/ सरकारी विनियामक निकायों द्वारा अनुमोदित किसी विश्वविद्यालय/ संस्थान/ बोर्ड से किसी भी विषय में एमसीए/ एमई/ एमटेक/ एमएससी. **अधिमान्य:** साइबर सुरक्षा या सूचना प्रौद्योगिकी में उन्नत डिग्री. **अधिमान्य प्रमाण पत्र इस प्रकार हैं:** सीआईएसएसपी, सीआईएसएम, सीआईएसए, सीसीएसपी, पीएमपी, एमबीए (प्रौद्योगिकी प्रबंधन)	**अनिवार्य:** ● साइबर परामर्श के रूप में कम से कम 8-10 वर्षों के अनुभव सहित 12+ वर्षों का समग्र अनुभव. **अधिमान्य:** ● घरेलू और वैश्विक सुरक्षा मानकों के अनुरूप और बीएफएसआई क्षेत्र–केंद्रित व्यावसायिक मॉडल के अनुरूप साइबर सुरक्षा सलाहकार की भूमिका में कार्य करने या प्रबंधन का अनुभव. ● आईटी कंपनियों, बीएफएसआई संस्थानों, सरकारी साइबर सुरक्षा प्रतिष्ठानों, परामर्शदात्री संगठनों या संबंधित क्षेत्रों में साइबर सुरक्षा भूमिकाओं में अनुभव, जहाँ उम्मीदवार ने सूचना सुरक्षा, साइबर नीति, नवाचार, साइबर रक्षा या संबंधित क्षेत्रों में कार्य किया हो. ● किसी उत्कृष्टता केंद्र (सीओई) की स्थापना या उसमें कार्य करने का अनुभव.	● साइबर परामर्श के लिए विविध कौशल की आवश्यकता होती है, जिसमें मज़बूत नेतृत्व, रणनीतिक सोच, संप्रेषण और तकनीकी विशेषज्ञता शामिल है. ● हाल के खतरों और शोध के आधार पर सलाह तैयार करना. ● वैश्विक परिदृश्य में नियमित रूप से नज़र रखना और उनकी जाँच करना. ● हितधारकों की ज़रूरतों को पूरा करते हुए और जुड़ाव बढ़ाते हुए साइबर परामर्श कार्य को प्रभावी ढंग से चलाना. ● उसे संसाधनों का प्रभावी ढंग से प्रबंधन करना होगा, टीमों का नेतृत्व करना होगा और यह सुनिश्चित करना होगा कि शोध परियोजनाएँ संगठनात्मक लक्ष्यों के अनुरूप हों. ● साइबर सुरक्षा तकनीक की समझ और अनुभव तथा वस्तुनिष्ठ परिणाम देने के लिए सुरक्षा शोधकर्ताओं की टीम का नेतृत्व करने की क्षमता. ● उन्नत साइबर सुरक्षा प्रवृत्तियों, ख़तरा विश्लेषण, बाज़ार की समझ और महत्वपूर्ण विश्लेषण क्षमताओं की समझ. ● तेज़–तर्रार माहौल में रणनीतिक रूप से सोचने और नवाचार को आगे बढ़ाने की क्षमता. ● साइबर सलाहकार टीम प्रमुख संगठन को साइबर ख़तरों से बचाने, व्यावसायिक निरंतरता सुनिश्चित करने और एक मज़बूत साइबर सुरक्षा स्थिति बनाए रखने में एक प्रमुख नेता के रूप में कार्य करता है.

घ. जॉब प्रोफ़ाइल और मुख्य दायित्व क्षेत्र:

पद संख्या	पद	जॉब प्रोफ़ाइल	मुख्य दायित्व क्षेत्र
1	**सेंटर हेड (सीएच)**	भारतीय स्टेट बैंक के साइबर सुरक्षा उत्कृष्टता केंद्र के संचालन और कार्यान्वयन पहलुओं का नेतृत्व करना. उत्कृष्टता केंद्र के उद्देश्य तीन स्तंभों में विभाजित हैं: ● नीति विकास, विनियामक नीतियों और मानकों के लिए सहयोग और अत्याधुनिक साइबर सुरक्षा क्षमता का निर्माण. कार्यक्रम संयोजन और उद्योग एवं शिक्षा जगत के साथ सहयोग के माध्यम स प्रतिभा निर्माण. ● साइबर अनुसंधान और नवाचार को बढ़ावा देना. ● बीएफएसआई पारिस्थितिकी तंत्र को सुरक्षित करने और ग्राहकों की सुरक्षा के लिए सलाह प्रदान करना.	● उत्कृष्टता केंद्र की पहलों के संचालन और उनके दैनिक प्रबंधन के लिए प्रक्रियाओं को स्थापित और सुव्यवस्थित करना. ● यह सुनिश्चित करना कि उत्कृष्टता केंद्र बैंक द्वारा निर्धारित अपने लक्ष्यों और उद्देश्यों को प्राप्त करे. ● तत्काल, मध्यावधि और दीर्घकालिक कार्य योजनाओं की रणनीति बनाना और उन्हें परिभाषित करना, साथ ही उत्कृष्टता केंद्र के उद्देश्यों के अनुरूप कार्यक्रम पहलों को लागू करना और उन्हें बनाए रखना. ● प्रासंगिक घटनाक्रमों और ताज़ा खबरों के लिए वैश्विक साइबर सुरक्षा परिदृश्य की निगरानी करना. ● उत्कृष्टता केंद्र की सभी गतिविधियों को व्यवस्थित रूप से निष्पादित करने के लिए एक टीम को इकट्ठा करने के लिए कार्य करना. ● डिलीवरेबल्स की स्थिति पर नज़र रखना, विभिन्न स्तरों के हितधारकों को अपडेट प्रदान करना और आवश्यकतानुसार सुधारात्मक कार्रवाई करना. ● एसबीआई टीमों और शोध छात्रों, साइबर सुरक्षा उद्योग पारिस्थितिकी तंत्र, आरबीआई और साइबर सुरक्षा क्षेत्र में कार्यरत सरकारी एजेंसियों के साथ बातचीत करना ताकि यह सुनिश्चित हो सके कि उत्कृष्टता केंद्र बीएफएसआई क्षेत्र में नवाचार और अनुसंधान के लिए एक साइबर सुरक्षा प्रकाश स्तंभ के रूप में कार्य करता है.

2	**सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नीति एवं साइबर अकादमी**	साइबर नीति और साइबर अकादमी इकाई के सीनियर वाइस प्रेसिडेंट हमारे साइबर सुरक्षा उत्कृष्टता केंद्र के अंतर्गत साइबर सुरक्षा नीतियों और प्रशिक्षण कार्यक्रमों के विकास, कार्यान्वयन और प्रबंधन की देखरेख करेंगे.	● **मुख्य उत्तरदायित्व:** यह भूमिका यह सुनिश्चित करने में महत्वपूर्ण है कि साइबर उत्कृष्टता केंद्र की नीति केंद्र ऐसी नीतियों का समर्थन करे जो बैंकिंग उद्योग की साइबर सुरक्षा को मज़बूत करें और विनियामकों के साथ घनिष्ठ रूप से बातचीत करें. आदर्श उम्मीदवार में मज़बूत नेतृत्व क्षमता, साइबर सुरक्षा नियमों का व्यापक ज्ञान और अनुपालन पहलों को प्रभावी ढंग से प्रबंधित करने की सिद्ध क्षमता होगी. इस भूमिका के लिए छात्रों, व्यवसायियों, उद्योग विशेषज्ञों, शिक्षाविदों और अंतिम उपयोगकर्ताओं (ग्राहकों) जैसे विविध हितधारकों के लिए साइबर संबंधी प्रशिक्षणों की नवीनतम सामग्री को तैयार करना भी आवश्यक है. मुख्य उत्तरदायित्व : ● नेतृत्व और प्रबंधन: ● साइबर सुरक्षा उत्कृष्टता केंद्र के लक्ष्यों के अनुरूप नीति और अकादमी इकाई के लिए रणनीतिक दृष्टिकोण विकसित और कार्यान्वित करना. ● प्रशिक्षण समन्वयकों और नीति विश्लेषकों की टीम का नेतृत्व, मार्गदर्शन और प्रबंधन करना. ● इकाई के भीतर ईमानदारी, जवाबदेही और निरंतर सुधार की संस्कृति को बढ़ावा देना. ● ज्ञान के आदान–प्रदान के लिए उद्योग और नियामक मंचों की स्थापना और संचालन करना. **नीति विकास और कार्यान्वयन:** ● साइबर सुरक्षा नीतियों और प्रक्रियाओं की परिभाषा को आगे बढ़ाना ● नीति संरेखण और प्रभावशीलता सुनिश्चित करने के लिए आंतरिक और बाहरी हितधारकों के साथ सहयोग करना. **उद्योग सहभागिता और विचार नेतृत्व:** ● साइबर सुरक्षा नीति और अनुपालन से संबंधित उद्योग मंचों, सम्मेलनों और कार्य समूहों में संगठन का प्रतिनिधित्व करना. ● विनियामक निकायों, उद्योग भागीदारों और अन्य प्रासंगिक संस्थाओं के साथ संबंध बनाएँ और बनाए रखना. **शैक्षणिक सहयोग** ● अग्रणी विश्वविद्यालयों के साथ सहयोग करना. ● साइबर सुरक्षा क्षमता निर्माण के लिए पाठ्यक्रम डिज़ाइन और विकसित करना. ● हितधारकों की आवश्यकताओं और भूमिकाओं के आधार पर शिक्षण पद्धति को परिभाषित करना. ● उद्योग विशेषज्ञों और शिक्षाविदों के साथ सहयोग को बढ़ावा देना.
3	**सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर परामर्श**	साइबर परामर्श प्रमुख, साइबर सुरक्षा उत्कृष्टता केंद्र के अंतर्गत ख़तरे की ख़ुफ़िया जानकारी, नागरिक–केंद्रित पहलों और रणनीतिक परामर्श कार्यों के विकास, कार्यान्वयन और प्रबंधन की देखरेख करेंगे. आदर्श उम्मीदवार में मज़बूत नेतृत्व क्षमता, साइबर सुरक्षा क्षेत्रों का व्यापक ज्ञान और परामर्श पहलों को प्रभावी ढंग से प्रबंधित करने की सिद्ध क्षमता होगी.	● **रणनीतिक नेतृत्व:** साइबर परामर्श इकाई के लिए एक रणनीतिक दृष्टिकोण विकसित और कार्यान्वित करना जो साइबर उत्कृष्टता केंद्र के समग्र लक्ष्यों के अनुरूप हो. ● एक साइबर डिफेंस और ख़तरा ख़ुफ़िया जानकारी अभ्यास स्थापित करना जो साइबर सुरक्षा अभ्यासों में अग्रणी रहे. ● **ग्राहक जागरूकता कार्यक्रमों के लिए रणनीति का विकास:** ग्राहक/ नागरिक जागरूकता कार्यक्रमों के डिज़ाइन, कार्यान्वयन और निरंतर सुधार की देखरेख करना. ● **साझेदारी और सहयोग:** रणनीतिक सलाह को बेहतर बनाने के लिए शैक्षणिक संस्थानों, उद्योग जगत के नेताओं और सरकारी एजेंसियों के साथ साझेदारी स्थापित करना और उसे बनाए रखना. ● **गुणवत्ता आश्वासन:** कार्यक्रम की प्रभावशीलता के मूल्यांकन हेतु प्रक्रियाओं को लागू करना, जिसमें साइबर सुरक्षा क्षमताएँ और उसके अनुप्रयोग शामिल हों. ● **परिचालन उत्कृष्टता:** (i) यह सुनिश्चित करना कि प्रभावी संसाधन आवंटन और परियोजना प्रबंधन पद्धतियों के साथ परिचालन कुशल हों. (ii) अधिकतम प्रभाव के लिए संसाधनों का इष्टतम उपयोग सुनिश्चित करते हुए बजट का प्रबंधन करना.
4	**सीनियर वाइस प्रेसिडेंट (एसवीपी) – साइबर नवाचार और अनुसंधान**	नवाचार एवं अनुसंधान लैब के सीनियर वाइस प्रेसिडेंट हमारे साइबर सुरक्षा उत्कृष्टता केंद्र के अंतर्गत अनुसंधान एवं नवाचार प्रयासों का नेतृत्व एवं प्रबंधन करेंगे.	➢ **मुख्य उत्तरदायित्व** आदर्श उम्मीदवार एक दूरदर्शी नेता होगा जिसकी साइबर सुरक्षा अनुसंधान में गहरी पृष्ठभूमि हो और जो अनुसंधानकर्ताओं और प्रौद्योगिकीविदों की टीम को प्रेरित करने की क्षमता रखता हो, और जिसकी निम्नलिखित प्रमुख ज़िम्मेदारियाँ होंगी: **नेतृत्व और रणनीति:** ● साइबर सुरक्षा उत्कृष्टता केंद्र के व्यापक लक्ष्यों के अनुरूप नवाचार और अनुसंधान प्रयोगशाला के लिए रणनीतिक दृष्टिकोण विकसित और कार्यान्वित करना. ● अनुसंधानकर्ताओं, विश्लेषकों और प्रौद्योगिकीविदों की एक बहु–विषयक टीम का नेतृत्व, मार्गदर्शन और प्रबंधन करना. ● प्रयोगशाला के भीतर नवाचार, सहयोग और उत्कृष्टता की संस्कृति को बढ़ावा देना. ● उत्कृष्टता केंद्र की पहलों के कार्यान्वयन को गति देना. **अनुसंधान एवं विकास:** ● उभरते साइबर सुरक्षा खतरों और प्रौद्योगिकियों पर केंद्रित अत्याधुनिक अनुसंधान परियोजनाओं के डिज़ाइन और कार्यान्वयन की देखरेख करना. ● नवाचार के प्रमुख क्षेत्रों की पहचान करना और साइबर सुरक्षा समाधानों की सीमाओं को आगे बढ़ाने वाली पहलों को आगे बढ़ाना. ● अनुसंधान एजेंडा को आगे बढ़ाने और प्रौद्योगिकी हस्तांतरण सुनिश्चित करने के लिए शिक्षाविदों, उद्योग भागीदारों और आंतरिक हितधारकों के साथ सहयोग करना.

			नवाचार प्रयोगशाला: ● अत्याधुनिक सुविधाओं को सुनिश्चित करने के लिए नवाचार और अनुसंधान प्रयोगशाला के डिज़ाइन को सक्षम बनाना. ● बुनियादी ढाँचा सक्षमता, परिचालन मॉडल, परिणाम मापन आदि सहित अनुसंधान और नवाचार गतिविधियों के लिए ढाँचा स्थापित करना. ● प्रयोगशाला के कार्यान्वयन और संचालन के लिए रणनीतिक और परिचालन संबंधों को आगे बढ़ाना. **नवाचार और समाधान विकास:** ● अनुसंधान निष्कर्षों को व्यावहारिक साइबर सुरक्षा समाधानों और रणनीतियों में परिवर्तित करना. ● उभरती प्रौद्योगिकियों और कार्यप्रणालियों का मूल्यांकन करना और उन्हें मौजूदा ढाँचों में एकीकृत करना. ● नई प्रौद्योगिकियों को प्रदर्शित करने के लिए प्रोटोटाइप/ टूलकिट और प्रूफ–ऑफ–कॉन्सेप्ट प्रदर्शनों के विकास को बढ़ावा देना. **विचार नेतृत्व:** ● साइबर सुरक्षा क्षेत्र में एक विचार नेता के रूप में कार्य करना, उद्योग सम्मेलनों, सेमिनारों और कार्यशालाओं में संगठन का प्रतिनिधित्व करना. ● प्रतिष्ठित पत्रिकाओं में अनुसंधान निष्कर्ष प्रकाशित करना और प्रमुख उद्योग आयोजनों में प्रस्तुति देना. ● शिक्षा जगत, उद्योग और सरकार के प्रमुख हितधारकों के साथ संबंध बनाना और उसे बनाए रखना. **परिचालन उत्कृष्टता:** ● सुनिश्चित करना कि प्रयोगशाला प्रभावी संसाधन आवंटन और परियोजना प्रबंधन प्रथाओं के साथ कुशलतापूर्वक संचालित हो. ● अनुसंधान पहलों और नवाचार परियोजनाओं की प्रगति की निगरानी करना और उसकी रिपोर्ट करना. ● अधिकतम प्रभाव के लिए संसाधनों का इष्टतम उपयोग सुनिश्चित करते हुए प्रयोगशाला के बजट का प्रबंध करना.
5	**डिप्टी वाइस प्रेसिडेंट – साइबर नीति हब**	साइबर सुरक्षा नीति केंद्र का प्रमुख एक रणनीतिक नेतृत्वकर्ता होता है जो एक मज़बूत साइबर सुरक्षा स्थिति स्थापित करके और उसे बनाए रखकर किसी संगठन की सूचना परिसंपत्तियों की सुरक्षा सुनिश्चित करता है. यह संगठन के कर्मचारियों को कंपनी की संवेदनशील जानकारी की सुरक्षा के लिए कार्य करने हेतु मार्गदर्शन प्रदान करता है. इस भूमिका में छात्रों, व्यवसायियों, उद्योग विशेषज्ञों, शिक्षाविदों और अंतिम उपयोगकर्ताओं (ग्राहकों) जैसे विविध हितधारकों के लिए साइबर संबंधी प्रशिक्षणों की नवीनतम सामग्री को तैयार करना भी शामिल है. संवेदनशील डेटा की सुरक्षा और सुरक्षित परिचालन वातावरण बनाए रखने में यह एक महत्वपूर्ण भूमिका है. नीति हब के प्रमुख साइबर सुरक्षा प्रोफेशनलों की एक टीम की देखरेख भी करेंगे और परिचालन प्रक्रियाओं में सुरक्षा उपायों की नीति को एकीकृत करने के लिए विभिन्न हितधारकों के साथ सहयोग करेंगे.	➢ **मुख्य उत्तरदायित्व:** ● नेतृत्व और प्रबंधन: ● साइबर सुरक्षा उत्कृष्टता केंद्र के लक्ष्यों के अनुरूप साइबर सुरक्षा नीति के लिए रणनीतिक दृष्टिकोण विकसित और कार्यान्वित करना. ● साइबर सुरक्षा नीति प्रसारकों और नीति विश्लेषकों की टीम का नेतृत्व, मार्गदर्शन और प्रबंधन करना. संस्था के भीतर ईमानदारी, जवाबदेही और निरंतर सुधार की संस्कृति को बढ़ावा देना. ● ज्ञान के आदान–प्रदान के लिए उद्योग और विनियामक मंचों की स्थापना और संचालन करना. **नीति विकास और कार्यान्वयन:** ● नीति संरेखण और प्रभावशीलता सुनिश्चित करने के लिए आंतरिक और बाहरी हितधारकों के साथ सहयोग करना. ● संगठनात्मक लक्ष्यों, विनियामक अनुपालन और उद्योग की सर्वोत्तम प्रथाओं के साथ संरेखण सुनिश्चित करना. **उद्योग जुड़ाव और विचार नेतृत्व:** ● साइबर सुरक्षा नीति और अनुपालन से संबंधित उद्योग मंचों, सम्मेलनों और कार्य समूहों में संगठन का प्रतिनिधित्व करना. ● विनियामक निकायों, उद्योग भागीदारों और अन्य प्रासंगिक संस्थाओं के साथ संबंध बनाना और उसे बनाए रखना. **रणनीतिक नेतृत्व:** ● साइबर सुरक्षा नीति हब टीम का नेतृत्व करना और उत्कृष्टता केंद्र के नेतृत्व के लिए प्राथमिक नीति सलाहकार के रूप में कार्य करना. ● नीतियों को व्यावहारिक, प्रवर्तनीय और संरेखित बनाने के लिए आंतरिक विभागों (कानूनी, जोखिम, अनुपालन, आईटी, मानव संसाधन, आदि) के साथ सहयोग करना. ● साइबर सुरक्षा नीति अपनाने और जागरूकता से संबंधित परिवर्तन प्रबंधन पहलों को आगे बढ़ाना.
6	**डिप्टी वाइस प्रेसिडेंट – साइबर अकादमी**	साइबर सुरक्षा उत्कृष्टता केंद्र (CSCoE) के अंतर्गत साइबर अकादमी प्रमुख का कार्य साइबर सुरक्षा प्रशिक्षण कार्यक्रमों के विकास और क्रियान्वयन का नेतृत्व करना है, जिसमें पाठ्यक्रम विकास, प्रशिक्षक प्रशिक्षण और छात्र मूल्यांकन शामिल हो सकते हैं. इस भूमिका में रणनीतिक योजना, संसाधन प्रबंधन और हितधारक जुड़ाव भी शामिल होगा ताकि एक कुशल साइबर सुरक्षा कार्यबल के निर्माण में अकादमी की सफलता सुनिश्चित हो सके. प्रमुख जिम्मेदारियों में अकादमी के पाठ्यक्रम विकास की देखरेख, प्रशिक्षण वितरण का प्रबंधन और सभी साइबर सुरक्षा शिक्षा पहलों की गुणवत्ता और प्रभावशीलता सुनिश्चित करना शामिल है.	➢ **शैक्षणिक सहयोग:** ● अग्रणी विश्वविद्यालयों और अकादमियों के साथ जुड़ना. ● साइबर सुरक्षा क्षमता निर्माण के लिए पाठ्यक्रम तैयार करना और विकसित करना. ● हितधारकों की आवश्यकताओं और भूमिकाओं के आधार पर शिक्षण पद्धति को परिभाषित करना. ● उद्योग विशेषज्ञों और शिक्षाविदों के साथ सहयोग को बढ़ावा देना. ➢ **रणनीतिक योजना और नेतृत्व:** ● साइबर अकादमी के लिए रणनीतिक दृष्टिकोण, इसे साइबर सुरक्षा उत्कृष्टता केंद्र के समग्र लक्ष्यों के साथ संरेखित करना. ● एक व्यापक साइबर सुरक्षा प्रशिक्षण रोडमैप के विकास का नेतृत्व करना. ● अकादमी के पाठ्यक्रम को प्रासंगिक और अद्यतन बनाए रखने के लिए उद्योग की प्रवृत्तियों और उभरते खतरों पर विचार करना. ● प्रशिक्षण आवश्यकताओं और कमियों की पहचान करने के लिए हितधारकों के साथ सहयोग करना. ● तेजी से विकसित हो रहे तकनीकी परिदृश्य में बदलाव लाने की क्षमता के साथ रणनीतिक सोच. ● क्षमता निर्माण पहलों को डिजाइन और क्रियान्वित करने की क्षमता

			➢ **पाठ्यक्रम विकास एवं प्रबंधन:**
			● साइबर सुरक्षा प्रशिक्षण पाठ्यक्रमों, कार्यशालाओं और प्रमाणनों के डिज़ाइन, विकास और रखरखाव की देखरेख करना.
			● यह सुनिश्चित करना कि पाठ्यक्रम साइबर सुरक्षा विषयों की एक विस्तृत श्रृंखला को कवर करता हों, जिनमें शामिल हैं, लेकिन इन्हीं तक सीमित नहीं:
			  ● नेटवर्क सुरक्षा
			  ● क्लाउड सुरक्षा
			  ● घटना प्रतिक्रिया
			  ● डिजिटल फोरेंसिक
			  ● साइबर सुरक्षा प्रबंधन
			  ● प्रशिक्षण कार्यक्रमों में व्यावहारिक अभ्यास, सिमुलेशन और वास्तविक दुनिया के मामला अध्ययन शामिल करना.
			
			➢ **प्रशिक्षण वितरण और गुणवत्ता आश्वासन:**
			● उच्च-गुणवत्ता वाले शिक्षण अनुभव को सुनिश्चित करते हुए प्रशिक्षण कार्यक्रमों के वितरण का प्रबंधन करना.
			● प्रशिक्षकों और प्रशिक्षकों की एक टीम का पर्यवेक्षण और मार्गदर्शन करना.
			● आकलन, प्रतिक्रिया तंत्र और प्रदर्शन मेट्रिक्स के माध्यम से प्रशिक्षण कार्यक्रमों की प्रभावशीलता का मूल्यांकन करना.
			● प्रशिक्षण रिकॉर्ड और दस्तावेज़ीकरण बनाए रखना.
			
			➢ **सहयोग और हितधारक प्रबंधन:**
			● साइबर सुरक्षा वेंडरों और प्रशिक्षण प्रदाताओं जैसे बाहरी भागीदारों के साथ संबंध बनाना और उसे बनाए रखना.
			● उद्योग कार्यक्रमों और सम्मेलनों में साइबर अकादमी का प्रतिनिधित्व करना.

7	**डिप्टी वाइस प्रेसिडेंट – साइबर नवाचार और अनुकरण लैब**	उत्कृष्टता केंद्र (सीओई) के भीतर नवाचार एवं सिमुलेशन प्रयोगशाला का नेतृत्व करना, प्रयोग, प्रोटोटाइपिंग और अनुप्रयुक्त अनुसंधान की संस्कृति को बढ़ावा देना. यह भूमिका रणनीतिक नवाचार को आगे बढ़ाने, वास्तविक दुनिया की साइबर सुरक्षा और तकनीकी चुनौतियों का अनुकरण करने और संगठन की डिजिटल एवं साइबर क्षमताओं को भविष्य के लिए सुरक्षित बनाने हेतु उभरते समाधानों के विकास और परीक्षण में तेजी लाने पर केंद्रित है.	➢ **नवाचार रणनीति:** ● उत्कृष्टता केंद्र के लक्ष्यों और संगठन के समग्र साइबर सुरक्षा उद्देश्यों के अनुरूप एक व्यापक नवाचार रणनीति निर्धारित करना. ➢ **नवाचार प्रयोगशाला:** ● अत्याधुनिक सुविधाओं को सुनिश्चित करने के लिए नवाचार और अनुसंधान प्रयोगशाला के डिज़ाइन को सक्षम बनाना. ● बुनियादी संरचना सक्षमता, परिचालन मॉडल, परिणाम मापन आदि सहित अनुसंधान और नवाचार गतिविधियों के लिए ढाँचा स्थापित करना. ● प्रयोगशाला के कार्यान्वयन और संचालन के लिए रणनीतिक और परिचालन संबंधों को आगे बढ़ाना. ➢ **परिचालन उत्कृष्टता:** ● यह सुनिश्चित करना कि प्रयोगशाला प्रभावी संसाधन आवंटन और परियोजना प्रबंधन प्रथाओं के साथ कुशलतापूर्वक संचालित हो. ● अनुसंधान पहलों और नवाचार परियोजनाओं की प्रगति की निगरानी करना और उसे रिपोर्ट करना. ● अधिकतम प्रभाव के लिए संसाधनों का इष्टतम उपयोग सुनिश्चित करते हुए, प्रयोगशाला के बजट का प्रबंधन करना. ➢ **नवाचार और समाधान विकास:** ● अनुसंधान निष्कर्षों को व्यावहारिक साइबर सुरक्षा समाधानों और रणनीतियों में परिवर्तित करना. ● उभरती प्रौद्योगिकियों और कार्यप्रणालियों का मूल्यांकन और मौजूदा ढाँचों में एकीकृत करना. ● नई प्रौद्योगिकियों को प्रदर्शित करने के लिए प्रोटोटाइप/ टूलकिट और प्रूफ-ऑफ-कॉन्सेप्ट प्रदर्शनों के विकास को बढ़ावा देना. ➢ **उभरती प्रौद्योगिकियाँ:** ● उत्कृष्टता केंद्र (CoE) के लिए संभावित अनुप्रयोगों और अवसरों की पहचान करने हेतु कृत्रिम बुद्धिमत्ता, मशीन लर्निंग, ब्लॉकचेन और क्वांटम कंप्यूटिंग जैसी उभरती साइबर सुरक्षा तकनीकों पर अनुसंधान करना और उनका मूल्यांकन करना. ➢ **ज्ञान साझाकरण:** ● उत्कृष्टता केंद्र (CoE) के भीतर ज्ञान साझाकरण और सहयोग की संस्कृति को बढ़ावा देना, सर्वोत्तम प्रथाओं, अनुसंधान निष्कर्षों और सीखे गए सबक के प्रसार को सुगम बनाना. ➢ **बाहरी जुड़ाव:** ● नवीनतम प्रवृत्तियों से अवगत रहने और सहयोग को बढ़ावा देने के लिए उद्योग विशेषज्ञों, अनुसंधान संस्थानों और प्रौद्योगिकी वेंडरों सहित बाहरी हितधारकों के साथ संबंध बनाना और उसे बनाए रखना. ➢ **प्रतिभा विकास:** ● उत्कृष्टता केंद्र (CoE) के भीतर प्रतिभा की पहचान करना और उसका पोषण करना, नवाचार और साइबर सुरक्षा से संबंधित क्षेत्रों में व्यावसायिक विकास और वृद्धि के अवसर प्रदान करना. ➢ **प्रदर्शन मापन:** ● नवाचार पहलों की प्रभावशीलता और उत्कृष्टता केंद्र (CoE) के समग्र प्रभाव को मापने के लिए प्रमुख कार्य-निष्पादन संकेतक (KPI) परिभाषित करना और उन्हें ट्रैक करना. ➢ **सुरक्षा स्थिति में सुधार:** ● नवीन समाधानों और सर्वोत्तम प्रथाओं को अपनाकर संगठन की सुरक्षा स्थिति में निरंतर सुधार करना.

8	**डिप्टी वाइस प्रेसिडेंट – साइबर बेंचमार्किंग हब**	उत्कृष्टता केंद्र (सीओई) के भीतर बेंचमार्किंग हब का नेतृत्व करने के लिए, कार्यों, प्रक्रियाओं, प्रौद्योगिकियों और उद्योग के समकक्षियों के बीच डेटा–संचालित बेंचमार्किंग पहलों को बढ़ाने के लिए जिम्मेदार. भूमिका का उद्देश्य संरचित बेंचमार्किंग के माध्यम से प्रदर्शन अंतराल और सर्वोत्तम प्रथाओं की पहचान करके उत्कृष्टता, निरंतर सुधार और सूचित निर्णय लेने की संस्कृति को बढ़ावा देना है. यह एक मजबूत साइबर सुरक्षा बेंचमार्किंग कार्यक्रम की स्थापना और रखरखाव के लिए जिम्मेदार है. इस भूमिका में प्रमुख कार्य–निष्पादन संकेतकों (KPI) को परिभाषित करना, नियमित सुरक्षा आकलन करना और उद्योग की सर्वोत्तम प्रथाओं और समकक्षियों के समक्ष संगठन की साइबर सुरक्षा स्थिति की तुलना करना शामिल है. हब प्रमुख बेंचमार्किंग परिणामों के आधार पर साइबर सुरक्षा परिपक्वता और लचीलेपन में सुधार करने की पहल का भी नेतृत्व करेगा. सुरक्षा बेंचमार्किंग एक आधारभूत सुरक्षा प्रदर्शन स्थापित करने, समय के साथ परिवर्तनों और सुधारों को ट्रैक करने और समकक्षियों, प्रतियोगियों और विभिन्न व्यावसायिक इकाइयों के समक्ष प्रदर्शन की तुलना करने के लिए सरल, मात्रात्मक मैट्रिक्स का उपयोग करने का अभ्यास है.	➢ **बेंचमार्किंग कार्यक्रम का विकास और कार्यान्वयन:** ● इसमें प्रासंगिक मीट्रिक परिभाषित करना, उपयुक्त बेंचमार्किंग पद्धतियों का चयन करना और एक प्रक्रिया स्थापित करना शामिल है. ➢ **बेंचमार्क के समक्ष प्रदर्शन की तुलना:** ● उद्योग मानकों, सर्वोत्तम प्रथाओं और समकक्ष संगठनों के आधार पर मूल्यांकन परिणामों का विश्लेषण करके मज़बूती और कमज़ोरी के क्षेत्रों की पहचान करना. ➢ **सुधार योजनाएँ विकसित करना और उनका कार्यान्वयन:** ● बेंचमार्किंग निष्कर्षों के आधार पर, साइबर सुरक्षा की परिपक्वता और लचीलेपन में सुधार के लिए रणनीतियाँ विकसित और कार्यान्वित करना. ➢ **निरंतर सुधार की संस्कृति को बढ़ावा देना:** ● सकारात्मक बदलाव लाने के लिए बेंचमार्किंग डेटा का लाभ उठाकर साइबर सुरक्षा प्रथाओं में निरंतर सुधार की संस्कृति को बढ़ावा देना. ➢ **उद्योग के रुझानों के साथ अद्यतन रहना:** ● बेंचमार्किंग कार्यक्रम की प्रासंगिकता और प्रभावशीलता सुनिश्चित करने के लिए नए खतरों, तकनीकों और सर्वोत्तम प्रथाओं सहित विकसित हो रहे साइबर सुरक्षा परिदृश्य की निरंतर निगरानी करना.
9	**डिप्टी वाइस प्रेसिडेंट – साइबर अनुसंधान**	साइबर सुरक्षा उत्कृष्टता केंद्र (CSCoE) के लिए अनुसंधान एवं विचार नेतृत्व प्रमुख साइबर सुरक्षा में नवाचार और विशेषज्ञता को बढ़ावा देने पर फोकस करता है. इस भूमिका में अनुसंधान पहलों का नेतृत्व करना, विचार नेतृत्व सामग्री विकसित करना और संगठन के भीतर और बाहर साइबर सुरक्षा उत्कृष्टता की संस्कृति को बढ़ावा देना शामिल है. वे उभरते साइबर सुरक्षा खतरों और सर्वोत्तम प्रथाओं पर संगठन के दृष्टिकोण को आकार देने और व्यापक साइबर सुरक्षा विमर्श में योगदान देने के लिए ज़िम्मेदार होते हैं. यह भूमिका उन व्यक्तियों के लिए आदर्श है जिनमें साइबर सुरक्षा के प्रति जुनून, एक मजबूत अनुसंधान पृष्ठभूमि और साइबर सुरक्षा परिदृश्य पर महत्वपूर्ण प्रभाव डालने की इच्छा हो.	➢ **विचार नेतृत्व:** ● साइबर सुरक्षा क्षेत्र में एक विचार नेता के रूप में कार्य करना, उद्योग सम्मेलनों, सेमिनारों और कार्यशालाओं में संगठन का प्रतिनिधित्व करना. प्रतिष्ठित पत्रिकाओं में अनुसंधान निष्कर्ष प्रकाशित करना और प्रमुख उद्योग कार्यक्रमों में प्रस्तुति देना. ● शिक्षा जगत, उद्योग और सरकार के प्रमुख हितधारकों के साथ संबंध स्थापित करना और उसे बनाए रखना. ➢ **अनुसंधान पहलों का नेतृत्व करना:** ● उभरते खतरों, उद्योग की प्रवृत्तियों और संगठनात्मक आवश्यकताओं के आधार पर अनुसंधान क्षेत्रों की पहचान और प्राथमिकताएँ निर्धारित करना. ● भेद्यता विश्लेषण, खतरे की खुफिया जानकारी और सुरक्षा तकनीकों सहित साइबर सुरक्षा विषयों पर गहन अनुसंधान करना. ● साइबर सुरक्षा जोखिमों और समाधानों के मूल्यांकन के लिए अनुसंधान पद्धतियों और ढाँचों का विकास करें. ➢ **विचार नेतृत्व सामग्री विकसित करना:** ● साइबर सुरक्षा विषयों पर श्वेत पत्र, ब्लॉग पोस्ट, लेख और प्रस्तुतियों जैसी उच्च–गुणवत्ता वाली, व्यावहारिक सामग्री को परिभाषित करना. ● उद्योग प्रकाशनों, सम्मेलनों और ऑनलाइन प्लेटफ़ॉर्म सहित विभिन्न माध्यमों से शोध निष्कर्षों और विचार नेतृत्व सामग्री का प्रसार करना. ● संगठन को साइबर सुरक्षा मुद्दों पर एक अग्रणी प्राधिकरण के रूप में स्थापित करना. ➢ **साइबर सुरक्षा उत्कृष्टता की संस्कृति को बढ़ावा देना:** ● सीएससीओई और व्यापक संगठन के भीतर निरंतर सीखने, ज्ञान साझा करने और सहयोग की संस्कृति को बढ़ावा देना. ● अनुसंधान पद्धतियों, साइबर सुरक्षा सर्वोत्तम प्रथाओं और विचार नेतृत्व विकास पर टीम के सदस्यों को सलाह और मार्गदर्शन देना. ● नवीन साइबर सुरक्षा समाधानों और तकनीकों को अपनाने के लिए प्रोत्साहित करना. ➢ **हितधारकों के साथ जुड़ना:** ● उद्योग विशेषज्ञों, शिक्षाविदों, सरकारी एजेंसियों और अन्य साइबर सुरक्षा पेशेवरों सहित प्रमुख हितधारकों के साथ संबंध स्थापित करना. ● उद्योग कार्यक्रमों, सम्मेलनों और कार्यशालाओं में संगठन का प्रतिनिधित्व करना. ● साइबर सुरक्षा मानकों और सर्वोत्तम प्रथाओं के विकास में योगदान देना. ➢ **साइबर सुरक्षा में अनुसंधान को बढ़ावा देना:** ● उभरती प्रौद्योगिकियों और साइबर सुरक्षा पर उनके संभावित प्रभाव की खोज करना. ● साइबर सुरक्षा क्षमताओं को बढ़ाने के लिए नई प्रौद्योगिकियों का लाभ उठाने के अवसरों की पहचान करना. ● उभरती साइबर सुरक्षा चुनौतियों का समाधान करने के लिए नवीन समाधान विकसित करना.

10	**डिप्टी वाइस प्रेसिडेंट – साइबर डिफेंस एवं इंटेलिजेंस**	साइबर डिफेंस एवं इंटेलिजेंस प्रमुख किसी संगठन की साइबर सुरक्षा रणनीति और संचालन की देखरेख और प्रबंधन करता है, जिसमें खतरे का पता लगाने, घटनाओं पर प्रतिक्रिया देने और खुफिया जानकारी एकत्र करने पर ध्यान केंद्रित किया जाता है. इस भूमिका के लिए मज़बूत नेतृत्व, साइबर सुरक्षा में तकनीकी विशेषज्ञता और रणनीतिक लक्ष्यों को कार्यान्वयन योग्य योजनाओं में बदलने की क्षमता आवश्यक है. इसमें एक टीम का निर्माण और प्रबंधन, सुरक्षा नीतियों और प्रक्रियाओं का विकास और कार्यान्वयन, खतरे की खुफिया जानकारी का विश्लेषण करना और साइबर घटनाओं पर प्रतिक्रिया देना शामिल है. साइबर खतरे की खुफिया जानकारी को व्यापक सुरक्षा और व्यावसायिक उद्देश्यों के साथ संरेखित करें. यह एक नेतृत्वकारी भूमिका है जो किसी संगठन की सूचना प्रणालियों और डेटा को साइबर खतरों से बचाने पर केंद्रित होती है.	➢ **रणनीतिक योजना:** ● वैश्विक साइबर डिफेंस एवं इंटेलिजेंस कार्यक्रम को परिभाषित एवं उन्नत करना. ● संगठन के समग्र व्यावसायिक उद्देश्यों के साथ संरेखित करते हुए, उत्कृष्टता केंद्र की साइबर डिफेंस एवं इंटेलिजेंस रणनीति का विकास एवं क्रियान्वयन करना. ➢ **खतरे की खुफिया जानकारी एवं साइबर रक्षा:** ● प्रभावी खतरे का पता लगाना, घटना प्रतिक्रिया और भेद्यता प्रबंधन सुनिश्चित करना. ● साइबर सुरक्षा जोखिमों, घटनाओं और शमन योजनाओं के संबंध में सीनियर प्रबंधन, व्यावसायिक इकाइयों और अन्य हितधारकों के साथ प्रभावी ढंग से संवाद करना. ● उभरते खतरों और कमजोरियों की पहचान करने के लिए विभिन्न स्रोतों से खतरे की खुफिया जानकारी की निगरानी, विश्लेषण और प्रसार करना. ● मूल कारण और हमलावर के तरीकों की पहचान करने के लिए साइबर घटनाओं की फोरेंसिक जाँच करना. ➢ **हितधारक प्रबंधन:** ● साइबर सुरक्षा प्रयासों के संरेखण और समन्वय को सुनिश्चित करने के लिए आईटी, जोखिम प्रबंधन और कानूनी जैसे अन्य विभागों के साथ सहयोग करना. ➢ **टीमों का नेतृत्व और प्रबंधन:** ● इसमें साइबर सुरक्षा संचालन, घटना प्रतिक्रिया, ख़तरे की खुफिया जानकारी और सुरक्षा इंजीनियरिंग टीमों की देखरेख शामिल है. ➢ **साइबर रक्षा:** ● उन्नत मैलवेयर और फ़ोरेंसिक कौशल ● मैलवेयर और फ़ोरेंसिक लैब का डिज़ाइन और कार्यान्वयन ➢ **सुरक्षा संरचना:** ● संगठन की डिजिटल परिसंपत्तियों की सुरक्षा के लिए मज़बूत सुरक्षा संरचनाओं और प्रणालियों का डिज़ाइन, कार्यान्वयन और रखरखाव. ➢ **ख़तरे का पता लगाना और रोकथाम:** ● विभिन्न उपकरणों और तकनीकों का उपयोग करके संभावित ख़तरों के लिए वातावरण की सक्रिय रूप से निगरानी करना और निवारक उपायों को लागू करना. ➢ **घटना प्रतिक्रिया:** ● घटना प्रतिक्रिया योजनाओं और प्रक्रियाओं को परिभाषित करना और उन्हें बनाए रखना और साइबर सुरक्षा घटनाओं की प्रतिक्रिया का नेतृत्व करना.
11	**डिप्टी वाइस प्रेसिडेंट – साइबर नागरिक केंद्रित पहल**	● संगठनात्मक लक्ष्यों के अनुरूप नागरिक–केंद्रित पहलों का नेतृत्व, डिज़ाइन और कार्यान्वयन करना, यह सुनिश्चित करना कि सेवाएँ सुलभ, समावेशी, कुशल और प्रभावशाली हों. इस भूमिका के लिए रणनीतिक सोच, मज़बूत हितधारक जुड़ाव, कार्यक्रम प्रबंधन क्षमताएँ और डिजिटल एवं भौतिक अभिशासन पहलों में नागरिकों की ज़रूरतों की गहरी समझ आवश्यक है. ● उत्कृष्टता केंद्र के अंतर्गत नागरिक–केंद्रित कार्यक्रमों के लिए विज़न और रोडमैप तैयार करना और उसका नेतृत्व करना.	➢ **साइबर सुरक्षा रणनीतियों का विकास और कार्यान्वयन:** ● इसमें साइबर अपराध, ऑनलाइन धोखाधड़ी और डेटा उल्लंघन जैसे साइबर खतरों से नागरिकों की सुरक्षा के लिए योजनाएँ बनाना और उन्हें क्रियान्वित करना शामिल है. ➢ **कार्यक्रम प्रबंधन:** ● नागरिक–केंद्रित परियोजनाओं की योजना, कार्यान्वयन और क्रियान्वयन की निगरानी करना, यह सुनिश्चित करना कि वे समय पर और बजट के भीतर पूरी हों. ● पहलों के निर्बाध एकीकरण और कार्यान्वयन को सुनिश्चित करने के लिए विभिन्न विभागों और टीमों के बीच समन्वय करना. ● परियोजना की प्रगति की निगरानी करना, संभावित जोखिमों और समस्याओं की पहचान करना और शमन रणनीतियों को लागू करना. ➢ **साइबर जागरूकता और साक्षरता को बढ़ावा देना:** ● नागरिकों को ऑनलाइन सुरक्षा, डिजिटल नागरिकता और ज़िम्मेदार ऑनलाइन व्यवहार के बारे में शिक्षित करना महत्वपूर्ण है. ➢ **सुरक्षित डिजिटल सेवाओं तक पहुँच सुनिश्चित करना:** ● सभी नागरिकों के लिए, उनकी तकनीकी विशेषज्ञता की परवाह किए बिना, सरकारी सेवाओं को सुलभ और सुरक्षित बनाने के लिए कार्य करना. ➢ **सहयोग को बढ़ावा देना:** ● एक सुरक्षित ऑनलाइन वातावरण बनाने के लिए कानून प्रवर्तन, प्रौद्योगिकी कंपनियों और गैर–लाभकारी संगठनों सहित विभिन्न हितधारकों के साथ काम करना. ➢ **टीम का नेतृत्व:** ● पहल के लक्ष्यों को प्राप्त करने के लिए साइबर सुरक्षा पेशेवरों की टीम का प्रबंधन और मार्गदर्शन करना. ➢ **तकनीकी विशेषज्ञता:** ● नागरिक–केंद्रित समाधानों के डिज़ाइन और कार्यान्वयन के लिए तकनीकी मार्गदर्शन और सहायता प्रदान करना. ● इंटरनेट ऑफ थिंग्स, स्मार्ट इंफ्रास्ट्रक्चर, साइबर सुरक्षा और ई–गवर्नेंस जैसे क्षेत्रों में उभरती तकनीकों और प्रवृत्तियों पर अद्यतन रहना. ● विशिष्ट नागरिक–संबंधी अनुप्रयोगों के लिए उपयुक्त तकनीकों का मूल्यांकन करना और उनकी सिफारिश करना.

12	डिप्टी वाइस प्रेसिडेंट – साइबर परामर्श	साइबर परामर्श प्रमुख एक सीनियर स्तर का प्रोफेशनल होता है जो साइबर सुरक्षा सलाह और समाधान प्रदान करने पर केंद्रित टीमों का नेतृत्व और प्रबंधन करता है, साइबर सुरक्षा के सभी पहलुओं पर संगठन को रणनीतिक मार्गदर्शन और समर्थन प्रदान करने के लिए जिम्मेदार टीम का नेतृत्व करता है.	➢ **रणनीतिक नेतृत्व:** ● साइबर परामर्श इकाई के लिए एक रणनीतिक दृष्टिकोण विकसित और कार्यान्वित करना जो साइबर उत्कृष्टता केंद्र के समग्र लक्ष्यों के अनुरूप हो. ● साइबर सुरक्षा और ख़तरा ख़ुफ़िया जानकारी के अभ्यास के लिए एक परामर्श कार्य स्थापित करना जो साइबर सुरक्षा प्रथाओं में अग्रणी रहे. ➢ **साझेदारी और सहयोग:** ● रणनीतिक सलाह को बेहतर बनाने के लिए शैक्षणिक संस्थानों, उद्योग जगत के नेताओं और सरकारी एजेंसियों के साथ साझेदारी स्थापित करना और उसे बनाए रखना. ➢ **साइबर सुरक्षा रणनीतियों का विकास और कार्यान्वयन:** ● इसमें एक व्यापक साइबर सुरक्षा रोडमैप को परिभाषित और बनाए रखना, उसे समग्र व्यावसायिक उद्देश्यों के साथ संरेखित करना और उसका प्रभावी कार्यान्वयन सुनिश्चित करना शामिल है. ➢ **जोखिम प्रबंधन:** ● नियमित जोखिम मूल्यांकन करना, कमज़ोरियों की पहचान करना और साइबर खतरों के जोखिम को कम करने के लिए शमन रणनीतियों को लागू करना. ➢ **अनुपालन:** ● प्रभावी प्रशासन और सुरक्षा नियंत्रणों के कार्यान्वयन के माध्यम से उद्योग मानकों (जैसे आईएसओ) और विनियामक अपेक्षाओं का पालन सुनिश्चित करना. ➢ **टीम नेतृत्व:** ● साइबर परामर्श टीम को मार्गदर्शन, परामर्श और प्रकार्य–निष्पादन प्रबंधन प्रदान करना, एक सहयोगात्मक और उच्च–कार्यनिष्पादन वातावरण को बढ़ावा देना. ➢ **हितधारक प्रबंधन:** ● एक एकीकृत और प्रभावी साइबर सुरक्षा दृष्टिकोण को बढ़ावा देने के लिए व्यावसायिक इकाइयों, आईटी विभागों और बाहरी भागीदारों सहित विभिन्न हितधारकों के साथ सहयोग करना. ➢ **वर्तमान से अपडेट रहना:** ● संगठन की सुरक्षा को मज़बूत और अपडेट बनाए रखने के लिए नवीनतम साइबर खतरों, कमज़ोरियों और सुरक्षा तकनीकों से अवगत रहना. ➢ **साइबर सुरक्षा जागरूकता को बढ़ावा देना:** ● कर्मचारियों को सुरक्षा की सर्वोत्तम प्रथाओं के बारे में शिक्षित करना और पूरे संगठन में सुरक्षा जागरूकता की संस्कृति को बढ़ावा देना.

टिप्पणियां: केआरए: कार्यग्रहण करने पर केआरए निर्धारित किए जाएंगे. ऊपर वर्णित कार्य की रूपरेखा उदाहरण रूप में हैं. बैंक द्वारा उपर्युक्त पदों के लिए ऊपर वर्णित भूमिका/कार्य के अलावा समय–समय पर अन्य कार्य सौंपे जा सकते हैं.

ङ. अवकाश:

संविदा (OEC) पर नियोजित प्रस्तावित अधिकारी वित्तीय वर्ष के दौरान 30 दिनों के अवकाश का हकदार होगा जो वास्तविक और उचित कारणों के लिए बैंक द्वारा प्रदान की जाएगी.

च. नोटिस अवधि:

संविदा को किसी भी समय, बिना किसी पूर्वाग्रह के, किसी भी पक्ष की ओर से 90 दिन का नोटिस देकर या उसके बदले में 90 दिन की वेतन राशि का भुगतान/सरेंडर करने पर समाप्त किया जा सकता है.

छ. साक्षात्कार के लिए कॉल लेटर:

साक्षात्कार के लिए कॉल लेटर/ सूचना ईमेल द्वारा भेजी जाएगी या बैंक की वेबसाइट पर अपलोड कर दी जाएगी. **कोई कागजी प्रति नहीं भेजी जाएगी.**

ज. चयन प्रक्रिया: चयन शॉर्टलिस्टिंग, साक्षात्कार और सीटीसी वार्ता पर आधारित 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. साक्षात्कार के लिए उम्मीदवारों को बुलाये जाने का बैंक का निर्णय अंतिम होगा. **इस संबंध में किसी पत्राचार पर विचार नहीं किया जाएगा.** शॉर्टलिस्ट किए गए उम्मीदवारों को साक्षात्कार के लिए बुलाया जाएगा.
- ❖ **साक्षात्कार:** साक्षात्कार 100 अंकों का होगा. साक्षात्कार में अर्हक अंक बैंक द्वारा तय किए जाएंगे. इस संबंध में कोई पत्राचार नहीं किया जाएगा.
- ❖ **सीटीसी बातचीत:** साक्षात्कार में प्राप्त अंकों के आधार पर तैयार की गई मेरिट सूची के क्रम में उम्मीदवारों के साथ सीटीसी बातचीत एक–एक करके की जाएगी.
- ❖ **मेरिट सूची:** चयन के लिए मेरिट सूची केवल साक्षात्कार में प्राप्त अंकों के अवरोही क्रम में तैयार की जाएगी. एक से अधिक उम्मीदवारों के एक समान निर्दिष्ट अंक पाने पर (निर्दिष्ट सीमा पर एक समान अंक होने पर), ऐसे उम्मीदवारों की रैंक उनकी आयु के आधार पर अवरोही क्रम में रैंक की जाएगी.

झ. आवेदन कैसे करें:

उम्मीदवारों की **एक्टिव 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://bank.sbi/careers/current-openings** पर उपलब्ध लिंक के माध्यम से अपना ऑनलाइन पंजीकरण करें और इन्टरनेट बैंकिंग/ डेबिट कार्ड/ क्रेडिट कार्ड 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 ('दस्तावेज़ अपलोड कैसे करें' के अंतर्गत) नहीं कर देता/देती.

iii. उम्मीदवार आवेदन को ध्यानपूर्वक भरें. आवेदन पूरी तरह से भरने के बाद ही उम्मीदवार 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 बन कर आ 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 जब पूरी तरह से भरा जाएगा तब उम्मीदवार को चाहिए कि वह इसे प्रस्तुत करें और ऑनलाइन शुल्क का भुगतान करें.

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

शुल्क भुगतान के लिए दिशानिर्देश:

i. सामान्य/ईडब्ल्यूएस/अन्य पिछड़ा वर्ग उम्मीदवारों के लिए आवेदन शुल्क और सूचना प्रभार (अप्रतिदेय) ₹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 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 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. **भुगतान किया गया आवेदन शुल्क किसी भी कारण से वापस नहीं लौटाया जाएगा, न ही इसे किसी अन्य परीक्षा या फिर भावी चयन के लिए समायोजित किया जाएगा.**

ञ. दस्तावेज़ों को अपलोड कैसे करें:

अ. अपलोड किए जाने वाले दस्तावेज़ों का विवरण:

i. नवीनतम फोटोग्राफ और हस्ताक्षर
ii. संक्षिप्त बायोडाटा (पीडीएफ)
iii. पहचान पत्र का प्रमाण (पीडीएफ)
iv. जन्म तिथि का प्रमाण (पीडीएफ)
v. एससी/एसटी/ईडब्ल्यूएस/ओबीसी-एनसीएल प्रमाणपत्र, पीडब्ल्यूबीडी प्रमाणपत्र (यदि लागू हो) (पीडीएफ) (इस विज्ञापन के पृष्ठ संख्या 13 से 16 में उपलब्ध प्रारूप)
vi. शैक्षणिक योग्यता: संबंधित अंक तालिका/डिग्री प्रमाणपत्र (पीडीएफ)
vii. अनुभव प्रमाण पत्र/ऑफर लेटर (पीडीएफ)
viii. फॉर्म-16/ऑफर लेटर/वर्तमान नियोक्ता से नवीनतम वेतन पर्ची (पीडीएफ)
ix. पिछले 3 महीनों का वेतन खाता विवरण (पीडीएफ में)
x. अनापत्ति प्रमाणपत्र (एनओसी) (यदि लागू हो) (पीडीएफ)
xi. बायोडाटा
xii. सीटीसी बातचीत फॉर्म (पीडीएफ में)

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 होता है, तो आप 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 करके समायोजित कर लें.

स. हस्ताक्षर फाइल का प्रकार/आकार:

i. आवेदक सफेद कागज पर काली पेन से हस्ताक्षर करें.
ii. हस्ताक्षर आवेदक स्वयं करे 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 पेज 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 लायक हैं.

य. फोटो/हस्ताक्षर/दस्तावेज़ों 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 आयकॅन 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 पिक्सल 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 हैं.
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 दस्तावेज़ 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 जाएगा.**

ट. 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 ब्यौरा 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 नियोजन के बाद भी पता चलती है, तो उसकी सेवाएं 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 का नियोजन बैंक की आवश्यकता के अनुसार चिकित्सकीय रूप से उपयुक्त घोषित किए जाने के अधीन है. इस तरह का नियोजन 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 को सक्रिय रखें.

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

viii. **जो उम्मीदवार सरकार/अर्ध–सरकारी कार्यालयों, राष्ट्रीयकृत बैंकों और वित्तीय संस्थानों सहित सार्वजनिक क्षेत्र के प्रतिष्ठानों और एसबीआई समूह की कंपनियों 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.**

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

x. 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 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 मात्र मुंबई और मुंबई स्थित न्यायालयों/न्यायाधिकरणों/फोरम पर ही की जा सकती हैं. किसी भी मुकदमे/विवाद की सुनवाई का एकल व एकमात्र अधिकार क्षेत्र मुंबई ही होगा.

xvi. बाहरी उम्मीदवारों को, जिन्हें चयनित सूची के बाद साक्षात्कार के लिए बुलाया जा सकता है, को वास्तविक यात्रा के आधार पर भारत में सबसे लघुतर मार्ग से हवाई (इकोनॉमी क्लास) किराया यात्रा की लागत या वास्तविक यात्रा की लागत (जो भी कम हो) की प्रतिपूर्ति की जाएगी. स्थानीय वाहन जैसे टैक्सी/कैब/निजी वाहन व्यय/किराया देय नहीं होगा. यदि 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. **बैंक किसी भी स्तर पर इस भर्ती प्रक्रिया को पूरी तरह से या किसी विशेष पद के लिए रद्द करने का अधिकार सुरक्षित रखता है.**

xviii. **साक्षात्कार के समय, उम्मीदवार को उसके विरुद्ध लंबित आपराधिक मामलों (यदि कोई हों) का विवरण देना आवश्यक होगा. 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 पूछताछ के लिए, कृपया बैंक की वेबसाइट (URL - https://bank.sbi/web/careers) पर उपलब्ध "CONTACT US/post your query" लिंक के माध्यम से हमसे संपर्क करें.

मुंबई
दिनांक: 25.08.2025

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

महाप्रबंधक
(आरपी एवं पीएम)

आवेदन कैसे करें

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

↓

नीचे स्क्रॉल करें और संबंधित विज्ञापन पर क्लिक करें

↓

विज्ञापन सं. CRPD/SCO/2025-26/08 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)