बाह्य परिपत्र सं. 33 / डॉस - 08 / 2020 06 फरवरी 2020

संदर्भ सं. राबैं. पॉल. प्रका. / 3184 / जे-1 / 2019-20

अध्यक्ष

सभी क्षेत्रीय ग्रामीण बैंक

महोदय / महोदया

क्षेत्रीय ग्रामीण बैंकों (आरआरबी) के लिए व्यापक साइबर सुरक्षा फ्रेमवर्क - <u>समयबद्ध कार्यान्वयन के लिए क्रमिक पद्धति</u>

कृपया 16 मार्च 2018 के हमारे परिपत्र राबैं. डॉस. प्रका. पॉल. सं. 4813/ जे– 1 / 2017-18 का संदर्भ लें जिसके माध्यम से बैंकों में साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन से संबन्धित दिशानिर्देश जारी किए गए थे. आगे और परीक्षण के बाद साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन की क्रमिक पद्धति तैयार की गई है.

2. क्षेत्रीय ग्रामीण बैंकों को उनके डिजिटल स्तर और भुगतान प्रणाली के परिदृश्य के साथ उनके पारस्परिक जुड़ाव के आधार पर चार स्तरों में श्रेणीकृत किया गया है. इन स्तरों को निम्नानुसार परिभाषित किया गया है:

स्तर	**मानदंड**	**विनियामक निर्धारण**	**अभ्युक्ति**
स्तर I	सभी आरआरबी	अनुबंध-I में निर्धारित स्तर I के नियंत्रण	नियंत्रणों के अतिरिक्त, बैंक साइबर सुरक्षा के वल्नरेबिलिटी सूचकांक (वीआईसीएस-विक्स) टूल (अनुबंध Iअ) का प्रयोग करते हुए साइबर सुरक्षा को लेकर अपनी तैयारी का परीक्षण कर सकते हैं.
स्तर II	वे सभी आरआरबी, जो केंद्रीय भुगतान प्रणाली के	अनुबंध-I में निर्धारित स्तर I के नियंत्रण **के**	अतिरिक्त नियंत्रणों में शामिल हैं: डाटा की क्षति

स्तर	मानदंड	विनियामक निर्धारण	अभ्युक्ति
	उप-सदस्य हैं और निम्नलिखित मानदंडों में से कम-से-कम किसी एक को पूरा करते हैं: 1. अपने ग्राहकों को इंटरनेट बैंकिंग सुविधा (व्यू-आधारित और ट्रांजैक्शन- आधारित में से कोई भी) देते हैं. 2. एप्लिकेशन (स्मार्ट फोन का उपयोग) के माध्यम से मोबाइल बैंकिंग सेवा देते हैं. 3. सीटीएस/ आईएमपीएस/ यूपीआई के प्रत्यक्ष सदस्य हैं.	**साथ-साथ** अनुबंध-II में निर्धारित स्तर II के नियंत्रण	को रोकने की रणनीति, फिशिंग के विरुद्ध नियंत्रण और महत्वपूर्ण एप्लीकेशनों के वीए/पीटी.
स्तर III	वे आरआरबी जो निम्नलिखित मानदंडों में से कम-से-कम किसी एक को पूरा करते हैं: 1. सीपीएस के प्रत्यक्ष सदस्य हैं. 2. जिनके पास अपना एटीएम स्विच है. 3. जिनके पास स्विफ्ट (SWIFT) इंटरफेस है.	स्तर I और II के नियंत्रण **के साथ-साथ** अनुबंध-III में निर्धारित स्तर III के नियंत्रण	अतिरिक्त नियंत्रणों में शामिल हैं: उन्नत तात्कालिक खतरे से सुरक्षा और उसका प्रबंधन, ट्रांजैक्शन का जोखिम-आधारित अनुप्रवर्तन.
स्तर	वे आरआरबी जो सीपीएस	स्तर I, II और III के	अतिरिक्त नियंत्रणों में

स्तर	मानदंड	विनियामक निर्धारण	अभ्युक्ति
IV	के प्रत्यक्ष सदस्य/ उप-सदस्य हैं और जो निम्नलिखित मानदंडों में से कम-से-कम किसी एक को पूरा करते हैं: 1. जिनके पास अपना एटीएम स्विच है **और** जिनके पास स्विफ्ट (SWIFT) इंटरफेस है. 2. जो डाटा सेंटर होस्ट करते हैं या अपने स्वयं के अथवा अपनी सहायक संस्थाओं के माध्यम से अन्य बैंकों को सॉफ्टवेयर सपोर्ट देते हैं.	नियंत्रण **के साथ-साथ** अनुबंध-IV में निर्धारित स्तर IV के नियंत्रण	शामिल हैं: साइबर सुरक्षा परिचालन केंद्र (सी-एसओसी) (अपना स्वयं का अथवा सेवा-प्रदाताओं के माध्यम से) की स्थापना, और उच्चतर उत्तरदायित्व की सूचना प्रौद्योगिकी (आईटी) और सूचना सुरक्षा (आईएस) गवर्नेंस फ्रेमवर्क की स्थापना, परिपत्र जारी होने की तारीख से छह माह के भीतर.

3. निदेशक बोर्ड अंतिम रूप से बैंक की सूचना सुरक्षा के लिए उत्तरदायी है और वह प्रभावी सूचना प्रौद्योगिकी (आईटी) और सूचना सुरक्षा (आईएस) गवर्नेंस सुनिश्चित करने में अग्रसक्रिय भूमिका निभाएगा. शीर्ष प्रबंध तंत्र की प्रमुख भूमिका होगी बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति को कार्यान्वित करना, साइबर सुरक्षा के लिए आवश्यक सांगठनिक प्रक्रियाएँ स्थापित करना और पर्याप्त साइबर सुरक्षा सुनिश्चित करने के लिए आवश्यक संसाधन उपलब्ध कराना.

4. क्षेत्रीय ग्रामीण बैंक ऊपर दी गई तालिका में उल्लिखित मानदंडों के आधार पर स्व-मूल्यांकन कर यह निर्धारित करेंगे कि वे किस स्तर के लिए उपयुक्त हैं और इसकी सूचना इस परिपत्र के जारी होने के 45 दिन के भीतर नाबार्ड के संबन्धित क्षेत्रीय कार्यालय को देंगे.

5. सभी क्षेत्रीय ग्रामीण बैंक इस परिपत्र के जारी होने से तीन महीने के भीतर **अनुबंध I** में निर्धारित नियंत्रण अपेक्षाओं का अनुपालन करेंगे. इसी प्रकार, स्तर II, III

और IV के क्षेत्रीय ग्रामीण बैंक क्रमश: **अनुबंध II, III और IV** में निर्धारित नियंत्रण अपेक्षाओं को लागू करेंगे.

6. क्षेत्रीय ग्रामीण बैंक स्वयं किए गए जोखिम और क्षमता आकलन के आधार पर सुरक्षा उपायों के उच्चतर स्तर को अपना सकते हैं. इसके अलावा, यदि किसी क्षेत्रीय ग्रामीण बैंक ने, चाहे उसकी आस्तियों की राशि कितनी भी क्यों न हो, साइबर सुरक्षा के ऐसे फ्रेमवर्क को अपनाया है जो उनके उपयुक्त स्तर से ऊपर के स्तर का है, तो उत्कृष्ट पद्धति के रूप में यह वांछनीय है कि वह विद्यमान गवर्नेंस संरचना को बनाए रखे.

7. साइबर सुरक्षा नियंत्रणों की स्थापना के लिए साइबर सुरक्षा फ्रेमवर्क हेतु वल्नरेबिलिटी सूचकांक (विक्स) का उपयोग मार्गदर्शक टूल के रूप में किया जा सकता है.

8. साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन की प्राथमिक ज़िम्मेदारी बैंक की ही है. अपने प्रायोजक बैंकों के साथ आईटी प्लेटफॉर्म शेयर करने वाले क्षेत्रीय ग्रामीण बैंक अपने प्रायोजक बैंक के परामर्श से हमारे परिपत्र में जारी सभी निर्धारित साइबर सुरक्षा नियंत्रणों की समीक्षा कर सकते हैं. साइबर सुरक्षा फ्रेमवर्क के परिप्रेक्ष्य में प्रायोजक बैंकों और क्षेग्रा बैंकों की भूमिकाओं और दायित्वों का प्रलेखीकरण कर क्षेग्रा बैंक के स्तर पर मेन्टेन किया जा सकता है.

9. जैसा कि 16 मार्च 2018 के हमारे परिपत्र में निर्दिष्ट किया गया है, सभी क्षेत्रीय ग्रामीण बैंकों को साइबर सुरक्षा से जुड़ी सभी घटनाएँ, चाहे वे सफल हुई हों या कोशिश भर रही हों, सीएसआईटीई कक्ष, नाबार्ड को ई-मेल (csite@nabard.org) द्वारा तुरंत रिपोर्ट करना है और उसकी एक प्रति नाबार्ड के संबन्धित क्षेत्रीय कार्यालय को परांकित करनी है. यदि साइबर सुरक्षा से जुड़ी कोई घटना न हुई हो/ खतरा न देखा गया हो तो तिमाही **शून्य** रिपोर्ट भेजी जानी चाहिए.

10. इस परिपत्र की एक प्रति निदेशक बोर्ड की आगामी बैठक में रखी जा सकती है.

11. कृपया पावती दें.

भवदीय

(के एस रघुपति)
मुख्य महाप्रबंधक

संलग्न: यथोक्त.