आरबीआई/डीपीएसएस/2024-25/123

सीओ.डीपीएसएस.ओवीआरएसटी.सं. एस447/06-26-002/2024-25

30 जुलाई, 2024

अध्यक्ष / प्रबंध निदेशक / मुख्य कार्यकारी अधिकारी
अधिकृत गैर-बैंक भुगतान प्रणाली परिचालक

महोदया / प्रिय महोदय,

गैर-बैंक भुगतान प्रणाली परिचालकों के लिए साइबर आघात-सहनीयता और डिजिटल भुगतान सुरक्षा नियंत्रण पर मास्टर दिशानिदेश

भुगतान प्रणालियों की सुरक्षा और संरक्षा भारतीय रिजर्व बैंक (आरबीआई) का एक प्रमुख उद्देश्य है। यह सुनिश्चित करने के लिए कि अधिकृत गैर-बैंक भुगतान प्रणाली परिचालक (पीएसओ) मौजूदा और उभरती सूचना प्रणालियों और साइबर सुरक्षा जोखिमों के प्रति आघात-सहनीय हैं, 08 अप्रैल, 2022 के मौद्रिक नीति वक्तव्य के हिस्से के रूप में जारी विकासात्मक और नियामक नीतियों पर वक्तव्य में यह घोषणा की गई थी कि आरबीआई भुगतान प्रणाली परिचालकों (पीओएस) के लिए साइबर आघात-सहनीयता और भुगतान सुरक्षा नियंत्रण पर निदेश जारी करेगा।

2. तदनुसार, 02 जून, 2023 को हितधारकों से टिप्पणियाँ/प्रतिक्रियाएँ माँगते हुए एक मसौदा मास्टर निदेश प्रकाशित किया गया था। प्राप्त प्रतिक्रिया के आधार पर, इन जोखिमों की पहचान, मूल्यांकन, निगरानी और प्रबंधन के लिए मजबूत शासन तंत्र को शामिल करते हुए सुनिश्चित निदेशों को जारी करने का निर्णय लिया गया है। निदेशों में सिस्टम आघात-सहनीयता सुनिश्चित करने के लिए आधारभूत सुरक्षा उपायों के साथ-साथ सुरक्षित और सुदृढ डिजिटल भुगतान लेनदेन को भी शामिल किया गया है। हालांकि, परिचालकों को नवीनतम सुरक्षा मानकों को अपनाने का प्रयास करना चाहिए। कार्ड, पूर्वदत्त भुगतान लिखत (पीपीआई) और मोबाइल बैंकिंग का उपयोग करके किए गए भुगतानों के

लिए सुरक्षा और जोखिम शमन उपायों पर मौजूदा निर्देश पूर्ववत लागू होते रहेंगे। दिशानिर्देशों की प्रयोज्यता में किसी भी विसंगति के मामले में, इस मास्टर निदेश में दिए गए निर्देश प्रबल होंगे।

3. ये निदेश भुगतान और निपटान प्रणाली अधिनियम, 2007 (2007 का अधिनियम 51) की धारा 18 के साथ धारा 10 (2) के तहत जारी किए गए हैं।

भवदीय,

(सुधांशु प्रसाद)

मुख्य महाप्रबंधक

अनुक्रमणिका	प्रष्ठ
खंड I – प्रारंभिक	4
परिचय	4
संक्षिप्त शीर्षक और प्रारंभ	4
प्रयोज्यता	5
उद्देश्य	5
खंड II – शासन नियंत्रण	5
साइबर सुरक्षा तैयारी	5
जोखिम मूल्यांकन और निगरानी	6
खंड III – आधारभूत सूचना सुरक्षा उपाय / नियंत्रण	5
वस्तु- सूची प्रबंधन	5
पहचान और पहुँच प्रबंधन	7
नेटवर्क सुरक्षा	8
एप्लिकेशन सुरक्षा जीवन चक्र	8
सुरक्षा परीक्षण	9
विक्रेता जोखिम प्रबंधन	9
डेटा सुरक्षा	10
पैच और परिवर्तन प्रबंधन जीवन चक्र	10
घटना प्रतिक्रिया	11
व्यवसाय निरंतरता योजना (बीसीपी)	11
एप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई)	12
कर्मचारी जागरूकता / प्रशिक्षण	12
क्लाउड सुरक्षा	13
अन्य सुरक्षा उपाय	13
खंड IV – डिजिटल भुगतान सुरक्षा उपाय / नियंत्रण	14
मोबाइल भुगतान	15
कार्ड भुगतान	16
पूर्वदत्त भुगतान लिखत	16
संक्षिप्त शब्द	17

गैर-बैंक भुगतान प्रणाली परिचालकों (पीएसओ) के लिए साइबर आघात-सहनीयता और डिजिटल भुगतान सुरक्षा नियंत्रण पर मास्टर दिशानिदेश

खंड I

प्रारंभिक

परिचय

1. भुगतान और निपटान प्रणाली अधिनियम, 2007 (पीएसएस अधिनियम) की धारा 18 के साथ पठित धारा 10 (2) के तहत प्रदत्त शक्तियों का प्रयोग करते हुए, भारतीय रिजर्व बैंक (आरबीआई, बैंक) इस बात से संतुष्ट है कि ऐसा करना सार्वजनिक हित में आवश्यक और समीचीन है, यहां निर्दिष्ट मास्टर निदेश जारी करता है।

संक्षिप्त शीर्षक और प्रारम्भ

2. इन मास्टर निदेशों को भारतीय रिज़र्व बैंक (गैर-बैंक पीएसओ के लिए साइबर आघात-सहनीयता और डिजिटल भुगतान सुरक्षा नियंत्रण) मास्टर निदेश, 2024 (मास्टर निदेश, निदेश) कहा जाएगा।

3. ये निदेश उसी दिन से प्रभावी हो जाएंगे जिस दिन इन्हें आरबीआई की आधिकारिक वेबसाइट पर ज़ारी किया जाएगा। आवश्यक अनुपालन संरचना को लागू करने के लिए पर्याप्त समय प्रदान करने के लिए, एक चरणबद्ध कार्यान्वयन दृष्टिकोण[1] निम्नानुसार निर्धारित किया गया है –

[1] भारतीय रिज़र्व बैंक द्वारा पहले जारी अनुदेशों में निर्धारित समय-सीमा पहले की तरह ही लागू रहेगी।

विनियमित संस्था	समयावधि
बड़े गैर-बैंक पीएसओ[2]	1 अप्रैल 2025
मध्यम गैर-बैंक पीएसओ[3]	1 अप्रैल 2026
छोटे गैर-बैंक पीएसओ[4]	1 अप्रैल 2028

प्रयोज्यता

4. इन निदेशों के प्रावधान सभी अधिकृत गैर-बैंक पीएसओ पर लागू होंगे।

5. पीएसओ के डिजिटल भुगतान पारिस्थितिकी तंत्र (जैसे भुगतान गेटवे, तृतीय पक्ष सेवा प्रदाता, विक्रेता, आदि) का भाग बनने वाली अनियमित संस्थाओं के साथ पीएसओ के संबंधों से उत्पन्न साइबर और प्रौद्योगिकी संबंधी जोखिमों को प्रभावी ढंग से पहचानने, निगरानी करने, नियंत्रित करने और प्रबंधित करने के लिए, पीएसओ आपसी सहमति के अधीन ऐसी अनियमित संस्थाओं द्वारा भी इन निदेशों का पालन सुनिश्चित करेंगे। इस संबंध में बोर्ड द्वारा अनुमोदित एक संगठनात्मक नीति स्थापित की जाएगी।

उद्देश्य

6. इन निदेशों का उद्देश्य साइबर आघात सहनीयता पर जोर देते हुए समग्र सूचना सुरक्षा तैयारियों के लिए एक ढांचा प्रदान करके पीएसओ द्वारा परिचालित भुगतान प्रणालियों की सुरक्षा में सुधार करना है।

---

[2] इन निदेशों के प्रयोजन के लिए, क्लियरिंग कॉरपोरेशन ऑफ इंडिया लिमिटेड (सीसीआईएल), नेशनल पेमेंट्स कॉरपोरेशन ऑफ इंडिया (एनपीसीआई), एनपीसीआई भारत बिल पे लिमिटेड, कार्ड भुगतान नेटवर्क, गैर-बैंक एटीएम नेटवर्क, व्हाइट लेबल एटीएम परिचालक (डब्ल्यूएलएओ), बड़े पीपीआई जारीकर्ता, ट्रेड रिसीवेबल्स डिस्काउंटिंग सिस्टम (टीआरईडीएस) परिचालक, भारत बिल भुगतान परिचालन संस्था (बीबीपीओयू) और भुगतान एग्रीगेटर (पीए) को बड़े गैर-बैंक पीएसओ माना जाता है।

[3] मनी ट्रांसफर सर्विस स्कीम (एमटीएसएस) के अंतर्गत क्रॉस-बॉर्डर (इन-बाउंड) मनी ट्रांसफर परिचालकों और मध्यम पीपीआई जारीकर्ताओं को मध्यम गैर-बैंक पीएसओ माना जाता है।

[4] छोटे पीपीआई जारीकर्ता और त्वरित धन अंतरण परिचालकों को छोटे गैर-बैंक पीएसओ माना जाता है।

प्राधिकृत गैर-बैंक पीपीआई जारीकर्ताओं को छोटे, मध्यम और बड़े में वर्गीकृत करना वित्तीय बाजार अवसंरचना (एफएमआई) और खुदरा भुगतान प्रणाली (आरपीएस) के लिए ओवरसाइट फ्रेमवर्क के अनुसार है। यदि कोई पीपीआई जारीकर्ता उच्च श्रेणी में चला जाता है, तो जिस श्रेणी में वह जाता है, उसकी समयसीमा लागू होगी। उदाहरण के लिए, यदि कोई छोटा (या मध्यम) पीपीआई जारीकर्ता मध्यम श्रेणी (या बड़ी) में चला जाता है, तो उसे नए वर्गीकरण के समय से दो (या एक) वर्ष की अवधि के भीतर इन निदेशों का अनुपालन करना होगा, जैसा भी मामला हो।

खंड II

शासन नियंत्रण

7. पीएसओ का निदेशक मंडल (बोर्ड) साइबर जोखिम और साइबर आघात सहनीयता सहित सूचना सुरक्षा जोखिमों पर पर्याप्त निगरानी सुनिश्चित करने के लिए जिम्मेदार होगा। हालाँकि, प्राथमिक निगरानी को बोर्ड की एक उप-समिति को सौंपा जा सकता है, जिसकी अध्यक्षता सूचना/साइबर सुरक्षा में अनुभव रखने वाले सदस्य द्वारा की जाएगी, जिसकी बैठक हर तिमाही में कम से कम एक बार होगी।

8. पीएसओ संभावित सूचना सुरक्षा जोखिमों के प्रबंधन के लिए बोर्ड द्वारा अनुमोदित सूचना सुरक्षा (आईएस) नीति तैयार करेगा, जिसमें भुगतान प्रणालियों से संबंधित सभी अनुप्रयोगों और उत्पादों के साथ-साथ उन जोखिमों का प्रबंधन शामिल होगा जो वास्तविक रूप से सामने आए हैं। नीति की वार्षिक समीक्षा की जाएगी। इसमें कम से कम, (i) बोर्ड / बोर्ड की उप-समितियों, वरिष्ठ प्रबंधन और अन्य प्रमुख कर्मियों की भूमिकाएँ और जिम्मेदारियाँ शामिल होंगी; (ii) साइबर सुरक्षा जोखिम की पहचान, आकलन, प्रबंधन और निगरानी के उपाय, जिसमें कर्मचारियों / हितधारकों के प्रशिक्षण और जागरूकता के लिए प्रक्रियाओं के साथ-साथ साइबर आघात सहनीयता सुनिश्चित करने के लिए विभिन्न प्रकार के सुरक्षा नियंत्रण भी शामिल होंगे।

साइबर सुरक्षा तैयारी

9. पीएसओ साइबर खतरों और साइबर हमलों का पता लगाने, उन्हें रोकने, उनका जवाब देने और उनसे उबरने के लिए एक अलग बोर्ड द्वारा अनुमोदित साइबर संकट प्रबंधन योजना (सीसीएमपी) तैयार करेगा। मार्गदर्शन के लिए सीईआरटी-इन / नेशनल क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (एनसीआईआईपीसी) / आईडीआरबीटी और अन्य एजेंसियों से प्रासंगिक दिशा-निर्देशों का संदर्भ लिया जा सकता है।

जोखिम मूल्यांकन और निगरानी

10. बोर्ड, साइबर सुरक्षा सहित सूचना सुरक्षा के क्षेत्रों में विशेषज्ञता वाले वरिष्ठ स्तर के कार्यकारी (जैसे मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ)) को आईएस नीति और साइबर आघात-सहनीयता ढांचे को लागू करने के और पीएसओ की समग्र आईएस स्थिति का निरंतर आकलन करने की जिम्मेदारी और जवाबदेही सौंपेगा।

11. पीएसओ संभावित जोखिम घटनाओं की पहचान करने के लिए उचित मुख्य जोखिम संकेतक (केआरआई) और सुरक्षा नियंत्रणों की प्रभावशीलता का आकलन करने के लिए मुख्य प्रदर्शन संकेतक (केपीआई) परिभाषित करेगा। इन केआरआई और केपीआई की निगरानी पैराग्राफ 7 में संदर्भित बोर्ड की उप-समिति द्वारा लगातार की जाएगी।

12. आईटी आकलन रिपोर्ट (जैसे सिस्टम ऑडिट, वीए/पीटी रिपोर्ट, आदि) को आईटी निरीक्षण के लिए जिम्मेदार उप-समिति के समक्ष उस बैठक में प्रस्तुत किया जाएगा, जो कि इस तरह की रिपोर्ट उपलब्ध होने के बाद तुरंत होने वाली होगी।

13. पीएसओ को नए उत्पाद/सेवाओं/प्रौद्योगिकियों के लॉन्च या मौजूदा उत्पाद/सेवाओं के बुनियादी ढांचे या प्रक्रियाओं में बड़े बदलाव करने से संबंधित साइबर जोखिम मूल्यांकन अभ्यास करना होगा। ऐसे मूल्यांकन से उत्पन्न होने वाले कार्य बिंदुओं को सीआईएसओ या समकक्ष कार्यकारी की देखरेख में लागू किया जाएगा।

खण्ड III

आधारभूत सूचना सुरक्षा उपाय / नियंत्रण

14. वस्तु- सूची प्रबंधन

(क) पीएसओ सभी प्रमुख भूमिकाओं, सूचना परिसंपत्तियों (अनुप्रयोग, डेटा, अवसंरचना, कार्मिक, सेवाएं, आदि), महत्वपूर्ण कार्यों, प्रक्रियाओं और तृतीय-पक्ष सेवा प्रदाताओं का रिकॉर्ड बनाए रखेगा और उनके उपयोग, गंभीरता और व्यावसायिक मूल्य के स्तरों को वर्गीकृत और प्रलेखित करेगा।

(ख) नेटवर्क संसाधनों, अंतर-संबंधों और निर्भरताओं, तथा अन्य सूचना परिसंपत्तियों के साथ डेटा प्रवाह का एक पूर्ण प्रक्रिया प्रवाह आरेख बनाया और बनाए रखा जाना चाहिए , जिसमें अन्य तृतीय-पक्ष प्रणाली भी शामिल हों।

(ग) परिसंपत्ति की जानकारी में अनिवार्य रूप से पहचानकर्ता, नेटवर्क पता, परिसंपत्ति का स्थान, परिसंपत्ति के मालिक का नाम और एंड ऑफ लाइफ सपोर्ट (ईओएलएस) शामिल होना चाहिए। सभी परिसंपत्तियों (हार्डवेयर या सॉफ्टवेयर) जो ईओएलएस के करीब पहुँच रही हैं, का मूल्यांकन किया जाना चाहिए ताकि बिना समर्थन वाली परिसंपत्ति के निरंतर उपयोग से जुड़े जोखिमों का मूल्यांकन किया जा सके।

15. पहचान और अभिगम प्रबंधन

(क) ऐसी नीतियां, प्रक्रियाएं और नियंत्रण स्थापित किए जाने चाहिए जो अभिगम विशेषाधिकारों के साथ-साथ अभिगम अधिकारों के प्रशासन को भी संबोधित करें।

(ख) पीएसओ के आईटी वातावरण तक पहुँच रखने वाले सभी व्यक्तियों को एक डिजिटल पहचान सौंपी जाएगी, जिसे समाप्ति तक बनाए रखा जाएगा और निगरानी की जाएगी।

(ग) सिस्टम/सॉफ्टवेयर/सेवाओं में डिफ़ॉल्ट प्रमाणीकरण सेटिंग्स को निष्क्रिय कर दिया जाएगा और लाइव वातावरण में रोल आउट करने से पहले उन्हें बदल दिया जाएगा।

(घ) प्रणालियों और विभिन्न वातावरणों (विकास, परीक्षण, उत्पादन, आदि) तक पहुँच आवश्यकता-आधारित, जानने की आवश्यकता-आधारित और न्यूनतम विशेषाधिकार[5] के सिद्धांत पर आधारित होना चाहिए।

(ङ) विशेषाधिकार प्राप्त खातों[6] का उपयोग बहु-कारक प्रमाणीकरण के साथ किया जाएगा और इसकी कड़ी निगरानी की जाएगी। रोटेशन नीति सहित उचित नियंत्रण लागू किए जाएंगे।

(च) निराकरणीय मीडिया और पोर्टेबल उपकरणों (जैसे स्मार्टफोन, लैपटॉप, आदि) के सुरक्षित उपयोग को सुनिश्चित करने के लिए श्वेतसूची / काली सूची में डालने के लिए केंद्रीकृत तंत्र सहित आवश्यक सुरक्षा नियंत्रण स्थापित किए जाएंगे।

(छ) दूरस्थ/घर से कार्य करने की स्थिति में, बहु-कारक प्रमाणीकरण तंत्र सहित पर्याप्त सावधानियां बरती जाएंगी।

(ज) पीएसओ ऐसी प्रक्रियाओं को परिभाषित और क्रियान्वित करेगा जो निष्क्रियता की पूर्व-निर्धारित अवधि के बाद सिस्टम और दूरस्थ सत्रों को सीमित, लॉक और समाप्त कर देती हैं।

(झ) पीएसओ को प्राकृतिक आपदाओं और अन्य खतरों से अपनी सूचना परिसंपत्तियों तक पहुँच की सुरक्षा के लिए समय-समय पर परीक्षण के साथ भौतिक और पर्यावरणीय सुरक्षा उपाय करने होंगे।

16. नेटवर्क सुरक्षा

पीएसओ अपने नेटवर्क और प्रणालियों को बाहरी खतरों से बचाने के लिए निम्नलिखित उपाय करेगा:

(क) नेटवर्क उपकरणों को सुरक्षा नियमों के लिए समय-समय पर कॉन्फ़िगर और जाँचा जाएगा;

(ख) सुरक्षा परिचालन केंद्र (एसओसी) एकत्रित व्यापक नेटवर्क और सिस्टम लॉग की सक्रिय और केंद्रीकृत निगरानी सुनिश्चित करेगा तथा सुरक्षा घटनाओं का पता लगाने, उन्हें बढ़ाने और त्वरित प्रतिक्रिया के लिए प्रभावी उपकरणों के साथ प्रबंधन सुनिश्चित करेगा;

(ग) स्वचालित तंत्र (जैसे सुरक्षा सूचना और घटना प्रबंधन (एसआईईएम) प्रणाली), जो बहुआयामी हमलों का पता लगाने के लिए अपने व्यावसायिक इकाइयों में सभी नेटवर्क और सिस्टम अलर्ट और किसी भी अन्य विषम गतिविधि को सहसंबंधित करता है, को स्थापित किया जाएगा;

---

[5] न्यूनतम विशेषाधिकार का सिद्धांत किसी उपयोगकर्ता या प्रक्रिया को केवल उन विशेषाधिकारों या विशिष्ट डेटा, संसाधनों और अनुप्रयोगों तक पहुंच प्रदान करने से संबंधित है जो इच्छित कार्य के लिए या आवश्यक कार्य को पूरा करने के लिए आवश्यक हैं।

[6] विशेषाधिकार प्राप्त खाते ऐसे उपयोगकर्ता खाते को कहते हैं जिसके पास सामान्य उपयोगकर्ता की तुलना में अधिक विशेषाधिकार होते हैं, जैसे कि व्यवस्थापक स्तर के खाते। ऐसे उपयोगकर्ता सॉफ़्टवेयर को इंस्टॉल या हटा सकते हैं, ऑपरेटिंग सिस्टम को अपग्रेड कर सकते हैं, या सिस्टम या एप्लिकेशन कॉन्फ़िगरेशन को संशोधित कर सकते हैं। उनके पास उन फ़ाइलों तक भी पहुँच हो सकती है जो आम तौर पर मानक उपयोगकर्ताओं के लिए सुलभ नहीं होती हैं।

(घ) मैलवेयर विरोधी समाधान लागू किए जाएंगे ताकि मैलवेयर के हमलों को रोका जा सके, उनका पता लगाया जा सके और उन्हें नियंत्रित किया जा सके, इसके लिए आने वाले सभी डेटा को स्कैन किया जाएगा ताकि मैलवेयर को सिस्टम में स्थापित होने और संक्रमित होने से रोका जा सके;

(ङ) नेटवर्क ट्रैफ़िक की कुशलतापूर्वक निगरानी करने और संगठन के अंदर और बाहर डेटा के प्रवाह को फ़िल्टर करने के लिए आईएस सिस्टम में बहु-स्तरीय सीमा सुरक्षा शामिल की जाएगी। असामान्य गतिविधियों/घटनाओं का पता लगाने और उन्हें ठीक करने के लिए पर्याप्त उपाय किए जाने चाहिए;

(च) भूमिका, स्थान और वातावरण (उत्पादन, परीक्षण, विकास, आदि) के आधार पर नेटवर्क विखंडन किया जाएगा ताकि अलग-अलग महत्वपूर्ण प्रणालियों और डेटा को अलग किया जा सके; यह सुनिश्चित करने के लिए श्वेतसूची समाधान लागू किए जाएंगे कि केवल मान्य आवश्यकताओं वाले अनुमत अनुप्रयोग और सेवाएँ ही चल रही हैं। निरंतर निगरानी के साथ पोर्ट की श्वेतसूची भी सुनिश्चित की जा सकती है; और

(छ) पीएसओ अपने नेटवर्क से उपकरणों (जैसे लैपटॉप, डेस्कटॉप, मोबाइल, आदि) को तभी कनेक्ट करने की अनुमति देंगे जब यह सुनिश्चित हो जाएगा कि वे निर्धारित सुरक्षा उपायों/आवश्यकताओं को पूरा करते हैं।

17. एप्लिकेशन सुरक्षा जीवन चक्र (एएसएलसी)

(क) पीएसओ उत्पादों/सेवाओं के डिजाइन और विकास के लिए सुरक्षित-सॉफ्टवेयर विकास जीवन चक्र (एस-एसडीएलसी) जैसे 'डिजाइन द्वारा सुरक्षित' दृष्टिकोण का पालन करेगा और यह सुनिश्चित करेगा कि निर्माण प्रक्रिया के दौरान कोई सुरक्षा कमजोरी न आए।

(ख) पीएसओ एक बहु-स्तरीय एप्लिकेशन आर्किटैक्चर को लागू करेगा, जो डिजिटल भुगतान उत्पादों और सेवाओं को विकसित करते समय डेटाबेस परत को अन्य परतों से अलग करना सुनिश्चित करेगा।

(ग) एएसएलसी दिशानिर्देश खरीदे गए उत्पादों/सेवाओं पर भी लागू होंगे। इसके अलावा, पीएसओ तृतीय पक्ष के विक्रेताओं से खरीदे गए सभी महत्वपूर्ण अनुप्रयोगों का स्रोत कोड प्राप्त करेगा। यदि स्रोत कोड प्राप्त करना संभव नहीं है, तो सेवाओं की निरंतरता सुनिश्चित करने के लिए स्रोत कोड के लिए एक एस्क्रो व्यवस्था स्थापित करनी होगी।

18. सुरक्षा परीक्षण

(क) पीएसओ यह सुनिश्चित करेगा कि उसके सभी अनुप्रयोगों को पर्याप्त आवृत्ति (कम से कम वार्षिक आधार पर) पर प्रमाणित मोड में योग्य प्रोफशनेल के माध्यम से सख्त सुरक्षा परीक्षण, जैसे स्रोत कोड समीक्षा, वीए, पीटी आदि के अधीन किया जाए।

(ख) यदि सोर्स कोड का स्वामित्व पीएसओ के पास नहीं है, तो उसे एप्लिकेशन डेवलपर से एक प्रमाणपत्र प्राप्त करना होगा, जिसमें यह बताया जाएगा कि एप्लिकेशन में कोई कमजोरियाँ, , मैलवेयर और कोड में कोई गुप्त चैनल नहीं है। स्रोत कोड में किसी भी बदलाव के लिए नया प्रमाणपत्र प्राप्त करना होगा।

(ग) सुरक्षा परीक्षण में रिपोर्ट की गई कमियों को समयबद्ध तरीके से हल किया जाएगा। किसी भी आवर्ती अवलोकन को पुनरावृत्ति और समाधान के लिए विस्तृत विश्लेषण के साथ आईटी निरीक्षण के लिए जिम्मेदार बोर्ड उप-समिति को रिपोर्ट किया जाना चाहिए।

(घ) महत्वपूर्ण कार्यों, अनुप्रयोगों और अवसंरचना घटकों का समर्थन करने वाली नई या मौजूदा सेवाओं का परिनियोजन या पुनर्नियुक्ति, वीए/पीटी सहित सुरक्षा ऑडिट करने और परिणामी टिप्पणियों को संबोधित करने के बाद ही किया जाना चाहिए।

19. विक्रेता जोखिम प्रबंधन

पीएसओ को आरबीआई द्वारा दिनांक 03 अगस्त, 2021 के परिपत्र (समय-समय पर अद्यतन) के तहत पीएसओ द्वारा भुगतान और निपटान संबंधी गतिविधियों की आउटसोर्सिंग के लिए जारी फ्रेमवर्क द्वारा निर्देशित किया जाएगा।

(क) पीएसओ विक्रेता परिवेश से अपने नेटवर्क में घुसपैठ को रोकने के लिए आवश्यक सुरक्षा नियंत्रण लागू करेगा।

(ख) पीएसओ को बुनियादी ढांचे तथा डेटा के प्रसंस्करण, भंडारण और उपयोग की भौगोलिक स्थिति से संबंधित प्रासंगिक कानूनी और नियामक आवश्यकताओं का पालन करना होगा और अपने विक्रेताओं द्वारा अनुपालन भी सुनिश्चित करना होगा।

(ग) महत्वपूर्ण प्रक्रियाओं और गतिविधियों[7] में शामिल विक्रेताओं के मामले में, पीएसओ विक्रेता की साइबर आघात-सहनीयता क्षमताओं पर एक स्वतंत्र लेखा परीक्षक से प्रमाणित आश्वासन प्राप्त करेगा।

20. डेटा सुरक्षा

(क) पीएसओ अपने पास या विक्रेता प्रबंधित सुविधाओं पर उपलब्ध डेटा के संबंध में व्यवसाय और ग्राहक जानकारी (पारगमन और स्थिर दोनों में) की गोपनीयता, अखंडता, उपलब्धता और संरक्षण के लिए एक व्यापक डेटा लीक रोकथाम नीति लागू करेगा, जो रखी गई / प्रेषित जानकारी की गंभीरता और संवेदनशीलता के अनुरूप होगी।

(ख) डेटा परिसंपत्तियों की ट्रेसबिलिटी (पता लगाने की योग्यता) और दृश्यता सुनिश्चित करने के लिए पीएसओ उपयुक्त तंत्र का उपयोग करेगा।

[7] महत्वपूर्ण प्रक्रियाएं, आरबीआई द्वारा 03 अगस्त, 2021 के परिपत्र (समय-समय पर अद्यतन)"पीएसओ द्वारा भुगतान और निपटान संबंधी गतिविधियों की आउटसोर्सिंग के लिए रूपरेखा" में परिभाषित हैं।

(ग) पीएसओ लागू मानकों के आधार पर सूचना सुरक्षा प्रबंधन प्रणाली (आईएसएमएस) का विकास और कार्यान्वयन करेगा।

(घ) एप्लिकेशन और डेटाबेस सुरक्षा नियंत्रण डेटा, विशेष रूप से व्यक्तिगत पहचान योग्य जानकारी (पीआईआई), की सुरक्षित हैंडलिंग, प्रोसेसिंग, भंडारण और सुरक्षा पर ध्यान केंद्रित करेंगे। पारगमन और स्थिर डेटा को डेटा अथवा चैनल एन्क्रिप्शन या दोनों के माध्यम से सुरक्षित किया जाएगा।

(ङ) कार्ड (डेबिट/क्रेडिट/प्रीपेड) डेटा संग्रहीत करने वाले पीएसओ को पीसीआई-डीएसएस दिशानिर्देशों का पालन करना होगा और पीसीआई-डीएसएस प्रमाणीकरण प्राप्त करना होगा।

(च) पीएसओ के पास आवश्यक प्रणालियां और प्रक्रियाएं होंगी, जिनके माध्यम से समय-समय पर (कम से कम छमाही आधार पर) बैकअप डेटा का परीक्षण किया जाएगा, ताकि लेन-देन या ऑडिट-ट्रेल्स की हानि के बिना पुनर्प्राप्ति सुनिश्चित की जा सके।

21. पैच और परिवर्तन प्रबंधन जीवन चक्र

(क) पीएसओ, ओईएम/अन्य स्त्रोतों द्वारा जारी प्रौद्योगिकी और सॉफ्टवेयर परिसंपत्तियों के पैच की पहचान करने और उन्हें लागू करने के लिए, एक प्रलेखित नीति और प्रक्रिया लागू करेगा।

(ख) सुरक्षा पैच को उनके रिलीज़ होने के बाद उचित समय सीमा के भीतर संबंधित सिस्टम और एप्लीकेशन पर लागू किया जाएगा। जाने-माने / रिपोर्ट किए गए हमलों से निपटने के लिए जारी किए गए महत्वपूर्ण पैच के मामले में, पीएसओ के पास पैच को तुरंत लागू करने के लिए एक तंत्र होना चाहिए।

(ग) प्रणाली, प्रौद्योगिकी, अनुप्रयोग, स्रोत कोड आदि में किसी भी परिवर्तन को मजबूत परिवर्तन प्रबंधन प्रक्रियाओं का उपयोग करके प्रबंधित किया जाएगा तथा यह सुनिश्चित किया जाएगा कि आईटी सेट-अप की समग्र अखंडता से समझौता न हो।

(घ) पैच और परिवर्तनों को अन्य वातावरणों (जैसे विकास, परीक्षण, आदि) में परीक्षण और सत्यापन के बाद ही उत्पादन वातावरण में लागू किया जाएगा।

22. घटना प्रतिक्रिया

(क) पीएसओ बोर्ड द्वारा अनुमोदित घटना प्रतिक्रिया तंत्र स्थापित करेगा, जिसमें साइबर घटनाओं के बारे में अपने वरिष्ठ प्रबंधन, संबंधित कर्मचारियों और नियामक, पर्यवेक्षी और संबंधित सार्वजनिक प्राधिकरणों को तुरंत सूचित करने के प्रावधान शामिल होंगे।

(ख) प्रतिक्रिया रणनीतियों में विभिन्न घटना परिदृश्यों से निपटने के लिए तत्परता शामिल होनी चाहिए, जो की परिस्थितिजन्य जागरूकता और संभावित प्रभाव, निरंतर संचार और हितधारकों के साथ समन्वय पर आधारित होगी।

(ग) घटना के बाद का विश्लेषण, जिसमें फोरेंसिक विश्लेषण (जहां भी आवश्यक हो) शामिल है, घटनाओं के प्रभाव और मूल कारण का पता लगाने के लिए किया जाएगा। ऐसी घटनाओं की पुनरावृत्ति से बचने के लिए पर्याप्त उपाय किए जाएंगे।

(घ) साइबर हमले, महत्वपूर्ण सिस्टम/इंफ्रास्ट्रक्चर में व्यवधान, आंतरिक धोखाधड़ी, निपटान में देरी आदि जैसी असामान्य घटनाओं की सूचना घटना रिपोर्टिंग प्रारूप (**अनुलग्नक 1**) में, पता लगने के 6 घंटे के भीतर, आरबीआई को दी जानी चाहिए। रिपोर्ट की जाने वाली घटनाओं के प्रकारों की सांकेतिक सूची **अनुलग्नक 2** में दी गई है। किसी भी साइबर सुरक्षा घटना की सूचना भी सीईआरटी-इन को दी जानी चाहिए।

23. व्यवसाय निरंतरता योजना (बीसीपी)

(क) पीएसओ विभिन्न साइबर खतरे परिदृश्यों के आधार पर एक बीसीपी विकसित करेगा, जिसमें चरम लेकिन संभावित घटनाएं शामिल होंगी, जिनसे वह प्रभावित हो सकता है। इसकी समीक्षा कम से कम साल में एक बार की जाएगी और इसमें साइबर सुरक्षा घटनाओं या घटनाओं के प्रबंधन के लिए एक व्यापक साइबर घटना प्रतिक्रिया, बहाली और पुनर्प्राप्ति योजना शामिल होगी।

(ख) बीसीपी को किसी भी प्रतिकूल घटना से तेजी से उबरने में सक्षम बनाने और प्रक्रियाओं और डेटा की सुरक्षा सुनिश्चित करते हुए महत्वपूर्ण संचालन की सुरक्षित बहाली को सक्षम करने के लिए डिज़ाइन किया जाएगा, जो की रिकवरी टाइम ऑब्जेक्टिव (आरटीओ) और रिकवरी पॉइंट ऑब्जेक्टिव (आरपीओ) के अनुरूप होगी।

(ग) पीएसओ लगभग शून्य आरपीओ प्राप्त करने का प्रयास करेगा।

(घ) पीएसओ प्राथमिक डेटा केंद्र (पीडीसी) से अलग भूकंपीय क्षेत्र में आपदा रिकवरी (डीआर) सुविधा स्थापित करेगा। डेटा के समाधान के लिए एक परिभाषित कार्यप्रणाली होगी ताकि यह सुनिश्चित किया जा सके कि डीआर से परिचालन फिर से शुरू करते समय कोई डेटा हानि न हो।

(ङ) डी.आर. ड्रिल (अभ्यास), अर्ध-वार्षिक या अधिक, लगातार आधार पर आयोजित किए जाएंगे। आर.टी.ओ. और आर.पी.ओ. से किसी भी विचलन का विश्लेषण किया जाएगा और कमी को तत्काल आधार पर सुधारा जाएगा।

24. एप्लिकेशन प्रोग्रामिंग इंटरफेस (एपीआई)

(क) असुरक्षित एपीआई से उत्पन्न होने वाले जोखिमों के विरुद्ध अनुप्रयोगों की सुरक्षा के लिए, पीएसओ अन्य बातों के साथ-साथ निम्नलिखित उपाय लागू करेगा:

(i) प्रमाणीकरण और प्राधिकरण – संचार एप्लिकेशन की पहचान स्थापित करना;

(ii) गोपनीयता – सुनिश्चित करें कि संदेश की सामग्री के साथ हस्तक्षेप न किया जाए;

(iii) अखंडता – संसाधनों को विश्वसनीय रूप से स्थानांतरित किया जाए; और

(iv) उपलब्धता और खतरे से सुरक्षा – आवश्यकता पड़ने पर एपीआई उपलब्ध हो; असामान्य[8] गतिविधियों की पहचान की जाए और निवारक कार्रवाई की जाए।

(ख) पीएसओ को एपीआई सुरक्षा पर प्रासंगिक मानकों और विश्व स्तर पर मान्यता प्राप्त ढांचे का पालन करना होगा।

25. कर्मचारी जागरूकता / प्रशिक्षण

(क) पीएसओ अपने कर्मचारियों और अपनी सूचना परिसंपत्तियों का प्रबंधन करने वाले विक्रेताओं के लिए सूचना सुरक्षा मुद्दों पर समय-समय पर दोहराए जाने वाले प्रशिक्षण/जागरूकता कार्यक्रम सुनिश्चित करेगा।

(ख) कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के आवधिक मूल्यांकन की प्रणाली चालू की जाएगी। बेंचमार्क स्कोर से कम जागरूकता स्तर वाले कर्मचारियों को सूचना परिसंपत्तियों तक पहुँचने से प्रतिबंधित/निषिद्ध किया जा सकता है।

(ग) बोर्ड के सदस्यों और प्रमुख वरिष्ठ प्रबंधन कार्मिकों को सूचना सुरक्षा और साइबर जोखिमों के संबंध में प्रशिक्षण दिया जाएगा तथा उन्हें संवेदनशील बनाया जाएगा।

26. क्लाउड सुरक्षा

(क) क्लाउड सेवाओं की सदस्यता लेने वाले पीएसओ को क्लाउड परिचालन नीति (बोर्ड द्वारा अनुमोदित सूचना सुरक्षा नीति के भाग के रूप में) लागू करनी होगी, जिसमें अन्य बातों के साथ-साथ क्लाउड सर्वर में स्थित की जा सकने वाली गतिविधियों, क्लाउड सेवा प्रदाता (सीएसपी) के लिए स्पष्ट रूप से पहचानी गई भूमिकाओं और जिम्मेदारियों, डेटा स्थानीयकरण, सुरक्षा और पुनर्प्राप्ति आवश्यकताओं पर प्रकाश डाला जाएगा।

(ख) यह सुनिश्चित किया जाएगा कि पीएसओ से संबंधित डेटा को स्पष्ट रूप से अलग किया जाए और सख्त एक्सेस कंट्रोल (पहुँच नियंत्रण) उपायों को लागू किया जाए। मल्टी-टेनेंसी वातावरण को डेटा अखंडता और गोपनीयता जोखिमों से, और डेटा के सह-मिश्रण से संरक्षित किया जाएगा।

[8] वह गतिविधि जो ऐतिहासिक गतिविधि से पर्याप्त रूप से भिन्न हो।

(ग) पीएसओ यह सुनिश्चित करेगा कि सीएसपी को समय-समय पर (कम से कम वार्षिक) स्वतंत्र सूचना और साइबर सुरक्षा ऑडिट करना होगा। ऐसी ऑडिट रिपोर्ट और सीएसपी के समग्र प्रदर्शन, इसकी साइबर आघात-सहनीयता क्षमताओं की वार्षिक समीक्षा बोर्ड उप-समिति द्वारा की जाएगी, जो की आईटी देखरेख के लिए जिम्मेदार है।

27. अन्य सुरक्षा उपाय

(क) पीएसओ यह सुनिश्चित करेगा कि सभी भुगतान लेनदेन, नकदी निकासी सहित, जिनमें इलेक्ट्रॉनिक मोड (बैंक खाते / डेबिट कार्ड / क्रेडिट कार्ड / पीपीआई, आदि) के माध्यम से खाते में डेबिट शामिल है, केवल बहु-कारक प्रमाणीकरण के माध्यम से सत्यापन के बाद ही अनुमित हो, सिवाय जहां स्पष्ट रूप से अनुमति / छूट दी गई हो।

(ख) पीएसओ को अपने संपूर्ण आईटी बुनियादी ढांचे का सुरक्षित विन्यास सुनिश्चित करना होगा। यह अपने सर्वर को पर्याप्त सुरक्षा उपायों से भी सुसज्जित करेगा ताकि अनधिकृत/धोखाधड़ी वाले लेनदेन न किए जा सकें और प्रमाणीकरण प्रक्रिया मजबूत, सुरक्षित और केंद्रीकृत हो।

(ग) पीएसओ संदिग्ध लेनदेन व्यवहार की पहचान करने और अलर्ट जारी करने के लिए वास्तविक समय/लगभग वास्तविक समय धोखाधड़ी निगरानी समाधान लागू करेगा।

(घ) पीएसओ के पास ग्राहकों द्वारा रिपोर्ट किए गए अनधिकृत/धोखाधड़ी वाले लेनदेन के त्वरित समाधान की सुविधा के लिए 24x7x365 आधार पर कार्य करने के लिए मानवयुक्त सुविधा होगी और साथ ही कानून प्रवर्तन एजेंसियों (एलईए) को त्वरित प्रतिक्रिया प्रदान की जाएगी।

(ङ) पीएसओ को ऑडिट लॉग को व्यवस्थित तरीके से कैप्चर, विश्लेषण, संग्रहीत और आर्काइव करने के लिए एक तंत्र स्थापित करना होगा। लॉग संदेश प्रासंगिक जानकारी प्रदान करेंगे जिससे कार्रवाई शुरू करने वाले उपयोगकर्ता, कार्रवाई और उस विशेष कार्रवाई के मापदंडों की विशिष्ट पहचान हो सके। लॉग डेटा तक पहुँच नियंत्रित आधार पर प्रदान की जाएगी। ऑडिट लॉग को कम से कम पाँच वर्षों की अवधि के लिए संरक्षित किया जाएगा।

(च) पीएसओ यह सुनिश्चित करेगा कि उनके द्वारा परिचालित भुगतान संरचना मजबूत, मापनीय और लेनदेन की मात्रा के अनुरूप हो; इसकी समीक्षा बोर्ड की उप-समिति द्वारा की जाएगी।

(छ) पीएसओ सुरक्षित मेल और संदेश प्रणाली का उपयोग करेगा ताकि यह सुनिश्चित किया जा सके कि मेल, संदेश या किसी अन्य मीडिया के माध्यम से आने-जाने वाला ट्रैफ़िक सुरक्षित है।

(ज) फिशिंग वेबसाइटों/रॉग एप्लिकेशनों की पहचान करने और उन्हें समाप्त करने के लिए पीएसओ को एंटी-फिशिंग/एंटी-रॉग ऐप सेवाओं की सदस्यता लेनी होगी।

(झ) पीएसओ निरंतर आधार पर, सीधे या अपने प्रतिभागियों और सेवा प्रदाताओं के माध्यम से, डिजिटल भुगतान उत्पादों का उपयोग करते समय धोखाधड़ी और साइबर खतरों से बचाव के लिए एहतियाती उपायों पर सार्वजनिक जागरूकता पैदा करेगा।

खण्ड IV

डिजिटल भुगतान सुरक्षा उपाय / नियंत्रण

डिजिटल भुगतान लेनदेन के लिए पीएसओ पर लागू मौजूदा निर्देशों के अतिरिक्त, निम्नलिखित निर्देश भी लागू होंगे।

28. पीएसओ अपने सदस्यों/प्रतिभागियों को विभिन्न मापदंडों के आधार पर ऑनलाइन अलर्ट के लिए तंत्र उपलब्ध कराएगा, जैसे विफल लेनदेन, लेनदेन की गति, साथ ही नए खाते के मापदंडों (जैसे, अत्यधिक गतिविधि), समय क्षेत्र, भौगोलिक स्थिति, आईपी पते की उत्पत्ति (असामान्य पैटर्न, निषिद्ध क्षेत्र/नकली आईपी के संबंध में), व्यवहारिक बायोमेट्रिक्स, सुलह बिंदु से लेनदेन की उत्पत्ति, मोबाइल वॉलेट / मोबाइल नंबर / वीपीए पर लेनदेन जिन पर विशिंग या अन्य प्रकार की धोखाधड़ी दर्ज/रिकॉर्ड की गई हो, अस्वीकृत लेनदेन, बिना अनुमोदन कोड वाले लेनदेन आदि।

29. पीएसओ या भुगतान प्रणाली प्रतिभागियों द्वारा ग्राहकों को एसएमएस / ई-मेल अलर्ट या कोई अन्य अधिसूचना भेजते समय, निम्नलिखित को सुनिश्चित किया जाएगा –

(क) बैंक खाता संख्या / कार्ड संख्या / अन्य गोपनीय जानकारी को यथासंभव संशोधित / छिपाया जाएगा।

(ख) ऑनलाइन भुगतान लेनदेन में व्यापारी का नाम (ना की भुगतान गेटवे / एग्रीगेटर का) और राशि का उल्लेख किया जाएगा; निधि अंतरण के लिए, लाभार्थी का नाम और डेबिट राशि का। पीएसओ यह सुनिश्चित करेगा कि नाम वह हो जो प्राप्तकर्ता खाते का संचालन करने वाली इकाई की प्रणाली से लिया गया हो।

(ग) ऐसे मामलों में जहां ओटीपी प्रमाणीकरण का कारक है, पीएसओ यह सुनिश्चित करेगा कि अधिसूचना संदेश के अंत में ओटीपी का उल्लेख किया गया है और संदेश में विशिष्ट लेनदेन का भी उल्लेख किया गया है।

30. पीएसओ अपने मोबाइल एप्लीकेशन / वेबसाइट पर एक ऐसी सुविधा प्रदान करेगा जो ग्राहकों को आवश्यक प्रमाणीकरण के साथ धोखाधड़ी वाले लेनदेन की पहचान करने / चिह्नित करने में सक्षम बनाएगी ताकि भुगतान साधन जारीकर्ता को निर्बाध और तत्काल सूचना मिल सके। पीएसओ यह सुनिश्चित करेगा कि सिस्टम प्रतिभागियों द्वारा भी इस तरह की व्यवस्था प्रदान कि जाए।

मोबाइल भुगतान

31. मोबाइल भुगतान सेवा लेनदेन प्रदान करने / सुविधा प्रदान करने / प्रसंस्करण करने वाले पीएसओ को निम्नलिखित सुरक्षा अभयासों और जोखिम शमन उपायों का पालन करना होगा और यह भी सुनिश्चित करना होगा कि उसके भुगतान प्रणाली में प्रतिभागी इन निर्देशों का पालन करें:

(क) पीएसओ यह सुनिश्चित करने के लिए एक तंत्र स्थापित करेगा कि मोबाइल एप्लीकेशन (अनुप्रयोग) किसी भी विसंगति या अपवाद से मुक्त हो, जिसके लिए एप्लीकेशन को प्रोग्राम नहीं किया गया था।

(ख) पीएसओ यह सुनिश्चित करेगा कि ग्राहक के साथ बातचीत के दौरान एक प्रमाणित सत्र, उसके एन्क्रिप्शन प्रोटोकॉल के साथ, अक्षुण्ण बना रहे। किसी भी हस्तक्षेप के मामले में या ग्राहक द्वारा एप्लिकेशन बंद करने के मामले में, सत्र समाप्त कर दिया जाएगा, और प्रभावित लेनदेन को हल किया जाएगा या उलटा दिया जाएगा।

(ग) पीएसओ डिवाइस और सिम के साथ मोबाइल एप्लीकेशन की डिवाइस बाइंडिंग[9] / फिंगर प्रिंटिंग सुनिश्चित करेगा। यदि मोबाइल एप्लीकेशन एक नीति निर्धारित निर्दिष्ट अवधि से अधिक समय तक उपयोग में नहीं आता है, तो पीएसओ यह सुनिश्चित करेगा कि डिवाइस बाइंडिंग फिर से की जाए।

(घ) पीएसओ यह सुनिश्चित करेगा कि मोबाइल एप्लिकेशन पर ऑनलाइन सत्र एक निश्चित अवधि की निष्क्रियता के बाद स्वचालित रूप से समाप्त हो जाए और ग्राहकों को पुनः लॉगिन करने के लिए कहा जाए।

(ङ) जहां लागू हो, पीएसओ असफल लॉग-इन या प्रमाणीकरण प्रयासों की अधिकतम संख्या निर्धारित करेगा जिसके बाद मोबाइल एप्लिकेशन तक पहुंच अवरुद्ध हो जाएगी। अवरुद्ध उत्पाद / सेवा तक पहुंच को फिर से सक्रिय करने के लिए एक सुरक्षित प्रक्रिया होनी चाहिए। ग्राहक को असफल लॉग-इन या प्रमाणीकरण प्रयासों के बारे में तुरंत सूचित किया जाएगा।

(च) पीएसओ एक नियंत्रण तंत्र स्थापित करेगा, ताकि रिमोट एक्सेस एप्लीकेशन कि उपस्थिति (जहां तक संभव हो) की पहचान की जा सके तथा रिमोट एक्सेस के चालू रहने के दौरान मोबाइल भुगतान एप्लीकेशन तक पहुंच को प्रतिबंधित किया जा सके।

(छ) जब भी भुगतान साधन से जुड़े पंजीकृत मोबाइल नंबर या ईमेल आईडी में कोई बदलाव होता है, तो ऑनलाइन मोड / चैनलों के माध्यम से किसी भी भुगतान लेनदेन की अनुमति देने से पहले न्यूनतम 12 घंटे की कूलिंग अवधि सुनिश्चित करनी होगी।

कार्ड भुगतान

32. पीएसओ यह सुनिश्चित करेगा कि भुगतान या अन्य किसी कार्य के लिए कार्ड विवरण प्राप्त करने के लिए व्यापारियों के यहां स्थापित टर्मिनलों को पीसीआई-पी2पीई कार्यक्रम के तहत सत्यापित किया गया हो; कार्ड

[9] डिवाइस बाइंडिंग को अधिमानतः हार्डवेयर, सॉफ्टवेयर और सेवा सूचना के संयोजन के माध्यम से कार्यान्वित किया जाएगा।

भुगतान प्राप्त करने के लिए व्यापारियों के यहां स्थापित पिन प्रविष्टि वाले पीओएस टर्मिनलों (डबल स्वाइप टर्मिनलों सहित) को पीसीआई-पीटीएस कार्यक्रम द्वारा अनुमोदित किया होना चाहिए।

33. कार्ड नेटवर्क, कार्ड, बैंक पहचान संख्या (बीआईएन) और कार्ड जारीकर्ता स्तर पर लेनदेन सीमाओं के कार्यान्वयन की सुसाध्य करेगा। ऐसी सीमाएँ अनिवार्य रूप से कार्ड नेटवर्क स्विच पर ही निर्धारित की जाएँगी। कार्ड नेटवर्क 24x7x365 आधार पर अलर्ट तंत्र स्थापित करेंगे, जो किसी भी संदिग्ध घटना के मामले में कार्ड जारीकर्ता को सूचित करेगा। कार्ड नेटवर्क यह सुनिश्चित करेंगे कि ग्राहकों के कार्ड विवरण उनके किसी भी सर्वर स्थान पर एन्क्रिप्टेड रूप में संग्रहीत किए जाएँ। वे यह भी सुनिश्चित करेंगे कि पठनीय प्रारूप में कार्ड विवरणों का प्रसंस्करण सुरक्षित तरीके से किया जाए।

पूर्वदत्त भुगतान लिखत

34. पीपीआई जारीकर्ताओं को उपयोगकर्ताओं के साथ ओटीपी और लेनदेन अलर्ट को उनकी पसंद की भाषा में संप्रेषित करने के लिए प्रोत्साहित किया जाता है, जिसमें स्थानीय भाषाएं भी शामिल हैं।

35. पीपीआई जारीकर्ता – बैंक और गैर-बैंक – को पीपीआई पर ऐसी निधियों को इलेक्ट्रॉनिक रूप से लोड करने के बाद धन अंतरण और नकद निकासी के लिए उपयुक्त कूलिंग अवधि लागू करनी होगी।

परिवर्णी शब्द

एपीआई	एप्लिकेशन प्रोग्रामिंग इंटरफ़ेस
एएसएलसी	एप्लिकेशन सुरक्षा जीवन चक्र
एटीएम	स्वचालित टेलर मशीन
बीसीपी	व्यवसाय निरंतरता योजना
बिन	बैंक पहचान संख्या
सीसीएमपी	साइबर संकट प्रबंधन योजना
सर्टिफिकेट-इन	भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल
सीआईएसओ	मुख्य सूचना सुरक्षा अधिकारी
सीएसपी	क्लाउड सेवा प्रदाता
डीआर	आपदा रिकवरी
ईओएलएस	जीवन समर्थन का अंत
आईडीआरबीटी	बैंकिंग प्रौद्योगिकी में विकास और अनुसंधान संस्थान
आईपी	इंटरनेट प्रोटोकॉल
आईएस	सूचना प्रणाली
आईएसएमएस	सूचना सुरक्षा प्रबंधन प्रणाली
आईटी	सूचना प्रौद्योगिकी
केपीआई	मुख्य प्रदर्शन संकेतक
केआरआई	मुख्य जोखिम संकेतक
एलईए	कानून प्रवर्तन एजेंसी
एनसीआईआईपीसी	राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र
ओईएम	मूल उपकरण निर्माता
ओटीपी	वन टाइम पासवर्ड
पीसीआई	भुगतान कार्ड उद्योग
पीसीआई-डीएसएस	भुगतान कार्ड उद्योग-डेटा सुरक्षा मानक
पीसीआई-पी2पीई	भुगतान कार्ड उद्योग-पॉइंट टू पॉइंट एन्क्रिप्शन
पीसीआई-पीटीएस	भुगतान कार्ड उद्योग-पिन लेनदेन सुरक्षा
पीडीसी	प्राथमिक डेटा केंद्र
पिन	व्यक्तिगत पहचान संख्या
पीओएस	बिक्री के केंद्र
पीपीआई	पूर्वदत्त भुगतान लिखत
पीएसओ	भुगतान प्रणाली ऑपरेटर
पीएसएस	भुगतान और निपटान प्रणाली
पीटी	पैठ परीक्षण
आरबीआई	भारतीय रिजर्व बैंक
आरपीओ	पुनर्प्राप्ति बिंदु उद्देश्य
आरटीओ	पुनर्प्राप्ति समय उद्देश्य
एसडीएलसी	सॉफ्टवेयर विकास जीवन चक्र
एस-एसडीएलसी	सुरक्षित-सॉफ्टवेयर विकास जीवन चक्र
एसआईईएम	सुरक्षा सूचना और घटना प्रबंधन
सिम	ग्राहक पहचान मॉड्यूल
एसएमएस	लघु संदेश सेवा
एसओसी	सुरक्षा संचालन केंद्र
वीए	भेद्यता मूल्यांकन
वीपीए	वर्चुअल भुगतान पता
डब्लूएलएओ	व्हाइट लेबल एटीएम ऑपरेटर