भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

आरबीआय/2015-16/229

डीसीबीआर.बीपीडी.(पीसीबी/आरसीबी) परिपत्रक क्र. 6/19.51.026/2015-16 **नोव्हेंबर 05, 2015**

मुख्य कार्यकारी अधिकारी
सर्व प्राथमिक (नागरी) सहकारी बँका/
राज्य व केंद्रीय सहकारी बँका

महोदय/महोदया

सहकारी बँकांच्या ग्राहकांना इंटरनेट बँकिंगची सुविधा

कृपया, युसीबीच्या ग्राहकांना इंटरनेट बँकिंगच्या सुविधा ह्या विषयावरील आमचे परिपत्रक युबीडी.बीपीडी. (एससीबी).परिपत्रक क्र.1/09.18.300/2011-12 दिनांक सप्टेंबर 26, 2011 चा संदर्भ घ्यावा. त्यानुसार, काही निकष पूर्ण करणा-या अनुसूचित नागरी सहकारी बँकांना (युसीबी), आरबीआयची पूर्व मंजुरी घेऊन, त्यांच्या ग्राहकांना, व्यवहारात्मक सुविधेसह इंटरनेट बँकिंगची सुविधा देण्याची परवानगी देण्यात आली होती. आणि तसेच, युसीबींच्या ग्राहकांसाठी इंटरनेट बँकिंग (फक्त राहण्यासाठी) सुविधा ह्यावरील आमचे परिपत्रक युबीडी.बीपीडी. (पीसीबी).परिपत्रक क्र. 21/09.18.300/2014-15 दिनांक ऑक्टोबर 13, 2014 अनुसार, काही विशिष्ट अटी पूर्ण करणा-या युसीबींना, आरबीआयची मंजुरी घेतल्याशिवायही, केवळ पाहण्यासाठी सुविधा असलेल्या इंटरनेट बँकिंगसाठी परवानगी देण्यात आली आहे.

(2) राज्य सहकारी बँका (एसटीसीबी) आणि जिल्हा केंद्रीय सहकारी बँका (डीसीसीबी) ह्यांना, त्यांच्या ग्राहकांना इंटरनेट बँकिंगची सेवा देण्यास अद्यापपर्यंत परवानगी देण्यात आलेली नाही. अशी इंटरनेट बँकिंग सुविधा देण्यासाठीच्या परवानगीसाठी, काही एसटीसीबी/डीसीसीबींकडून विनंती केली गेली असल्याने, एसटीसीबी/डीसीसीबींनाही त्यांच्या ग्राहकांना इंटरनेट बँकिंग सुविधा देण्यास परवानगी देण्याचे ठरविण्यात आले आहे. त्यानुसार, युसीबींना देण्यात आलेल्या मार्गदर्शक तत्वांचे पुनरावलोकन केले गेले आणि युसीबींना ह्याबाबत दिलेली मागील मार्गदर्शक तत्वे रद्द करुन, त्याऐवजी, सर्व सहकारी बँकांसाठी एकसमान मार्गदर्शक तत्वे देण्यात आली आहेत. सर्व सहकारी बँकांना लागु असलेली सुधारित मार्गदर्शक तत्वे पुढीलप्रमाणे आहेत :

सहकारी बँक विनियमन विभाग, केंद्रीय कार्यालय, सी-7, पहला/ दूसरा मजला, बांद्रा कुर्लासंकुल, बांद्रा (पूर्व), मुंबई - 400 051
फोन: 022 - 26578300/ 26578100 ; फैक्स: 022 - 26571117 ; ई-मेल: cgmdcbrco@rbi.org.in

(1) इंटरनेट बँकिंग (व्हयु ओन्ली) सुविधा

(3) कोअर बँकिंग सोल्युशन (सीबीएस) अंमलात आणली असणा-या, व इंटरनेट प्रोटोकॉल व्हर्शन 6 (आयपीव्ही 6) चा अंगिकार केलेल्या आणि हया परिपत्रकाच्या जोडपत्र मध्ये विहित केलेल्या मार्गदर्शक तत्वांचे पालन करणा-या, परवानाप्राप्त अशा सर्व एसटीसीबी, डीसीसीबी व युबीसी, आता, आरबीआयची पूर्व मंजुरी न घेताही, त्यांच्या ग्राहकांना, इंटरनेट बँकिंग (व्हयु ओन्ली) सुविधा देऊ शकतात. हया व्हयु ओन्ली सुविधेखाली देऊ केलेल्या सेवेसाठी, दोन घटक असलेले सत्यांकन किंवा एकदाच दिलेला पासवर्ड (ओटीपी) ची आवश्यकता असल्यास, हया परिपत्रकाच्या जोडपत्र-2 मध्ये विहित केलेल्या लक्षणांचा (त्यांच्या सेवांना योग्य अशा) अंगिकार बँका करु शकतात.

(4) ही इंटरनेट बँकिंग (व्हयु ओन्ली) सुविधा, ग्राहकांना देऊ करणा-या सहकारी बँकांनी खात्री करुन घ्यावी की, ही सुविधा फक्त व्यवहारात्मक नसलेल्या सेवांसाठी (शिल्लक-विचारणा, शिल्लक किती ते पाहणे, खाते-विवरणपत्र डाऊनलोड करणे, चेक बुक पुरविण्याची विनंती इत्यादि) दिली जात आहे, आणि कोणतेही ऑनलाईन निधी हस्तांतरण व्यवहार केले जाणार नाहीत.

(5) ही इंटरनेट बँकिंग (व्हयु ओन्ली) सेवा सुरु केल्यानंतर एक महिन्याच्या आत, त्या सहकारी बँकांनी, हया सेवेची सुरुवात केली असल्याचे, आरबीआयच्या संबंधित कार्यालयाला (तसेच, एसटीसीबी/डीसीसीबींच्या बाबतीत नाबार्डलाही) कळविणे आवश्यक आहे.

(2) व्यवहारात्मक सुविधेसह इंटरनेट बँकिंग

(6) सीबीएसची अंमलबजावणी केलेल्या, तसेच इंटरनेट प्रोटोकॉल व्हर्शन 6 (आयपीव्ही 6) चा अंगिकार केला असणा-या, आणि पुढील निकष पूर्ण करणा-या, परवानाप्राप्त सर्व एसटीसीबी, डीसीसीबी व युसीबी, त्यांच्या ग्राहकांना, आरबीआयची पूर्व मंजुरी घेऊन व्यवहारात्मक सुविधेसह इंटरनेट बँकिंग देऊ करु शकतात.

(अ) सीआरएआर 10 टक्क्यांपेक्षा कमी नसावा

(ब) मागील वित्तीय वर्षाच्या 31 मार्च रोजी, निव्वळ मूल्य रु.50 कोटी किंवा अधिक असावे

(क) एकूण एनपीए 7% पेक्षा कमी आणि निव्वळ एनपीए 3% पेक्षा अधिक नसावा

(ड) त्या बँकेने सरलेल्या वित्तीय वर्षात नक्त नफा मिळविलेला असावा, आणि सर्वसमावेशकतेने गेल्या चार वित्तीय वर्षांपैकी किमान तीन वर्षांमध्ये नक्त नफा मिळविलेला असावा.

(ई) गेल्या/सरलेल्या आर्थिक वर्षामध्ये, त्या बँकेकडून सीआरआर/एसएलआर ठेवण्यात कसुरी झालेली नसावी

(फ) तिची अंतर्गत नियंत्रण प्रणाली सशक्त असावी आणि तिच्या संचालक मंडळात किमान दोन व्यावसायिक संचालक असावेत

(ग) विनियात्मक अनुपालनाबाबत, त्या बँकेची कामगिरी चांगली असावी आणि अर्ज केल्याच्या मागील दोन आर्थिक वर्षांमध्ये, आरबीआयच्या निदेश/मार्गदर्शक तत्वांचे उल्लंघन केल्याबद्दल त्या बँकेवर आर्थिक दंड केलेला नसावा.

(7) ह्या परिपत्रकाच्या जोडपत्र 1 व 2 मध्ये विहित केलेल्या मार्गदर्शक तत्वांचे पालन केले असून वर दिलेले निकष पूर्ण करणा-या, एसटीसीबी, डीसीसीबी व युसीबींना, व्यवहारात्मक सुविधेसह इंटरनेट बँकिंग देऊ करण्याची परवानगी दिली जाईल. ह्यासाठी, त्यासाठी इच्छुक एसटीसीबी, डीसीसीबी आणि युसीबींनी आपला अर्ज आरबीआयच्या संबंधित कार्यालयाकडे (एसटीसीबी व डीसीसीबीसाठी नाबार्ड मार्फत), पुढील कागदपत्रांसह करावा :

(1) संचालक मंडळाने इंटरनेट बँकिंगवर मंजुर केलेल्या धोरणाची प्रत आणि आरबीआयने विहित केलेल्या, आयटी व आयएस धोरणाच्या आवश्यकतांचे अनुसरण करण्यात आले असल्याबाबत, एका स्वतंत्र ऑडिटरचे (सीआयएसए प्रमाणित) प्रमाणपत्र

(2) त्या देऊ करत असलेल्या सेवा/उत्पादांमध्ये लक्षणीय बदल केला असल्यास त्याबाबत आरबीआयला कळविण्यासाठी शपथपत्र.

(3) व्यवसाय योजना, खर्च व नफा विश्लेषण, वापरलेले तंत्रज्ञान, व्यावसायिक भागीदार, तृतीय पक्ष असे सेवा-दाते, आणि जोखमी सांभाळण्यासाठी बँक अंगीकार करु इच्छित असलेल्या प्रणाली व नियंत्रण व्यवस्था, ह्यासारख्या कार्यकारी व्यवस्था.

(8) ती शाखा, सुरक्षा प्रणाली व कार्यरीतींमधील उल्लंघनाची किंवा बंद पडण्याची प्रत्येक बाब आरबीआयच्या संबंधित प्रादेशिक कार्यालयाला (आणि एसटीसीबी/डीसीसीबीच्या बाबतीत नाबार्डलाही) कळवील आणि ते कार्यालय तिच्या मतानुसार, अशा बँकांचे ऑडिट/तपासणी करावयाचे ठरवील.

(9) ग्राहकांना, इंटरनेट (व्ह्यु ओन्ली) सुविधा आधीपासूनच देत असणा-या एसटीसीबी/डीसीसीबींनी, ह्या मार्गदर्शक तत्वांनुसार, त्यांच्या प्रणालींचे पुनरावलोकन करावे, आणि हे परिपत्रक देण्याच्या एक महिन्याच्या आत, त्या देत असलेल्या सेवांचा प्रकार व ह्या मार्गदर्शक तत्वांचे कोठपर्यंत पालन केले आहे हे, आरबीआयच्या संबंधित प्रादेशिक कार्यालयाला (नाबार्ड मार्फत) कळवावे. ह्या मार्गदर्शक तत्वांचा भंग झाला असल्यास, त्याबाबतच्या कृतीयोजना अवलंबिण्याच्या कालावधीसह कळविण्यात यावा.

(10) आधीपासूनच इंटरनेट बँकिंगमार्फत व्यवहारात्मक सेवा देत असलेल्या, एसटीसीबी/डीसीसीबींना सांगण्यात येते की, त्यांनी ह्या परिपत्रकामधील सूचनांचे पालन करावे आणि त्यांच्या व्यवहार-साचा तसेच खर्च/लाभ ह्याबाबतची प्रक्षेपणे सादर करावीत. तसेच हे परिपत्रक दिले गेल्याच्या तारखेपासून एक महिन्याच्या आत रिझर्व बँकेच्या संबंधित प्रादेशिक कार्यालयाकडून पोस्ट फॅक्टो मंजुरी मिळवावी. असे अर्ज, नाबार्डच्या मार्फत, आरबीआयच्या प्रादेशिक कार्यालयाकडे सादर केले जावेत.

आपली विश्वासु

(सुमा वर्मा)
प्रधान मुख्य महाव्यवस्थापक
सोबत - वरीलप्रमाणे.

जोडपत्र - 1

सहकारी बँकांच्या ग्राहकांना द्यावयाच्या इंटरनेट बँकिंग सुविधेवरील मार्गदर्शक तत्वे.

त्यांच्या ग्राहकांना इंटरनेट बँकिंग सेवा देऊ इच्छिणा-या व परवानाप्राप्त असलेल्या एसटीसीबी/डीसीसीबींनी पुढील बाबींचे पालन करावे.

(1) त्या बँकेने, तिच्या संचालक मंडळाच्या मंजुरीने इंटरनेट बँकिंगसाठी एक धोरण तयार करावे.

(2) हे धोरण, त्या बँकेच्या सर्वसमावेशक माहिती तंत्रज्ञान व माहिती सुरक्षा धोरणामध्ये बसणारे असावे, आणि रेकॉर्ड्स व सुरक्षा-प्रणालींच्या गोपनीयतेबाबत खात्री करणारे असावे.

(3) अशा धोरणामध्ये, तुमचा ग्राहक जाणाबाबत अनुसरण्याच्या कार्यरीती स्पष्टपणे ठरविलेल्या असाव्यात.

(4) ह्या धोरणांमध्ये तंत्रज्ञान व सुरक्षा मानकांचा समावेश असावा, आणि ह्या जोडपत्रात दिल्यानुसार, वैधानिक, विनियामक व पर्यवेक्षणाबाबतच्या प्रश्नांचाही विचार/उपाय केलेला असावा.

(5) बँकांनी त्यांच्याकडे सशक्त अंतर्गत प्रणाली ठेवाव्यात, आणि अशी सेवा देण्यामधील कार्यकारी जोखमीही विचारात घ्याव्यात.

(6) ही सेवा देऊ करण्यापूर्वी ग्राहकांबाबत असलेल्या जोखमी, जबाबदा-या व दायित्वे ह्यांचे सुयोग्य प्रकटीकरण केले जावे.

त्यानुसार, बँकांद्वारे अंमलात आणण्यासाठी पुढील मार्गदर्शक तत्वे देण्यात येत आहेत.

(1) तंत्रज्ञान व सुरक्षा मानके

(ए) सहकारी बँकांकडे, त्यांच्या संचालक मंडळाने मंजुर केलेले, सुयोग्य असे, माहिती सुरक्षा धोरण असावे. माहिती तंत्रज्ञान विभाग (आय टी) आणि माहिती सुरक्षा (आय एस) विभाग ह्यांची कर्तव्ये स्पष्टपणे वेगवेगळी अशी दर्शविली जावीत. माहिती तंत्रज्ञान विभाग, प्रत्यक्षपणे संगणक प्रणाली स्थापित करेल. खास माहिती प्रणालीच्या सुरक्षेसाठी एक वेगळा माहिती सुरक्षा अधिकारी ठेवला जावा. ह्याशिवाय, एक माहिती प्रणाली ऑडिटर, माहिती प्रणालीचे ऑडिट करेल.

(बी) बँकांच्या संचालक मंडळाने मंजुर केलेल्या आयएस धोरणानुसार, स्पष्ट अशी भूमिका असलेल्या, एक नेटवर्क व डेटाबेस अधिका-याची नेमणुक बँकांनी करावी.

(सी) प्रणाली, ॲप्लिकेशन सॉफ्टवेअर, युटिलिटीज्, टेलिकम्युनिकेशन लाईन्स, लायब्ररीज्, सिस्टिम सॉफ्टवेअर इत्यादींसाठीचे लॉजिकल ॲक्सेस नियंत्रण ठेवलेले असावे.

(डी) इंटरनेट व बँकेची प्रणाली ह्यांच्यादरम्यान कोणतीही थेट जोडणी नसल्याची खात्री बँकांनी करुन घ्यावी.

(ई) प्रणाली/नेटवर्कमध्ये घुसखोरी टाळण्यासाठी बँकांकडे परिणामकारक सुरक्षा उपाय असावेत.

(एफ) फाईल ट्रान्स्फर प्रोटोकॉल (एफटीपी), टेलनेट ह्यासारख्या, ॲप्लिकेशन सर्व्हरवरील सर्व अनावश्यक सेवा, अकार्यक्षम केल्या जाव्यात. ॲप्लिकेशन सर्व्हरला, ई-मेल सर्व्हरपासून दूर ठेवले जावे.

(जी) मिळालेल्या संदेशांसह, सर्व कॉंप्युटर ॲक्सेसेसचे लॉगिंग केले जावे. सुरक्षेची उल्लंघने (शंका असलेली किंवा प्रयत्न केलेली) नोंदून ठेवली जावीत व त्याबाबत पाठपुरावा केला जावा. घुसखोरी व हल्ल्याच्या विरुध्द प्रणालींवर देखरेख ठेवण्यासाठी बँकेकडे साधने (टूल्स) असावीत. सुरक्षेमधील भंग टाळण्यासाठी ह्या साधनांचा नियमितपणे उपयोग केला जावा. बँकांनी, त्यांच्या सुरक्षा-पायाभूत सोयींचे व सुरक्षा धोरणांचे, नियमितपणे पुनरावलोकन करत रहावे, आणि त्यांच्या स्वतःच्या अनुभवानुसार व बदलत्या तंत्रज्ञानाचा विचार करुन त्यांचा जास्त उपयोग करावा.

(एच) माहिती सुरक्षा अधिकारी व माहिती प्रणाली ऑडिटर ह्यांनी, नियतकालिकतेने, त्या प्रणालीची घुसखोरी चाचणी घ्यावी. ह्यात पुढील गोष्टी असाव्यात :

(1) पासवर्ड-क्रॅकिंग साधनाचा वापर करुन पासवर्डसचा अंदाज करणे.

(2) प्रोग्राममधील बॅक डोअर ट्रॅप्स शोधणे.

(3) डिस्ट्रिब्युटेड डिनायल ऑफ सर्व्हिस (डीडीओएस) व डिनायल ऑफ सर्व्हिस (डीओएस) चे हल्ले करुन, प्रणाली ओव्हरलोड करण्याचा प्रयत्न करणे.

(4) सॉफ्टवेअरमध्ये (विशेषतः ब्राउझर व ई-मेल सॉफ्टवेअरमध्ये) काही सर्वसामान्यतः ज्ञात अशा त्रुटी/कमकुवतपणा आहे काय ह्याची तपासणी करणे.

(5) कोठपर्यंत घुसखोरी झाली आहे ह्याबाबतची चाचणी, बाहेरील तज्ञांद्वारेही (ह्यांना एथिकल हॅकर्स म्हटले जाते) करविली जावी.

(आय) प्रत्यक्ष प्रवेशाबाबतचे नियंत्रण (फिजिकल ॲक्सेस कंट्रोल) काटेकोरपणे अंमलात आणावे. अंतर्गत व बाह्य संभावित हल्ल्यांविरुध्द (थ्रेट्स) ठेवावयाच्या प्रत्यक्ष सुरक्षेमध्ये, सर्व माहिती प्रणाली व त्या ठेवल्या असलेल्या जागा/ठिकाणे ह्यांचा समावेश असावा.

(जे) डेटाचे बॅकिंग-अप करण्यासाठी, बँकांकडे सुयोग्य पायाभूत सोयी व वेळापत्रक (शेड्युल) असले पाहिजे. बँकेच्या सुरक्षा-धोरणात दिल्यानुसार दिलेल्या कालावधीमध्ये, व्यवहार न गमविता रिकव्हरीची खात्री

करण्यासाठी, बॅक-अप केलेल्या डेटाची नियतकालिक चाचणी केली जावी. डिझास्टर रिकव्हरी साईट्स स्थापन करुन, व्यवहारात सातत्य आणण्याची खात्री केली जावी. ह्या सुविधांचीही नियतकालिक चाचणी केली जावी.

(के) कायदेशीर हेतु विचारात घेता, सर्व ॲप्लिकेशन्सना रेकॉर्ड ठेवण्याची सुविधा असावी. मिळालेले व पाठविलेले सर्व संदेश, एनक्रिप्टेड व डिक्रिप्टेड स्वरुपात ठेवणे अत्यावश्यक असेल.

(एल) इंटरनेट बँकिंग सॉफ्टवेअर स्थापन करण्यापूर्वी/अंमलात आणण्यापूर्वी, बँकांनी त्यांच्या व्हेंडरांकडून/सेवा दात्यांकडून, एकात्मतेचे/सचोटीची वचनपत्र घ्यावे.

(एम) सर्वसामान्यतः/नेहमीच्या कार्यकृतींसाठी, प्रणाली व ॲप्लिकेशन्सचा वापर करण्यापूर्वी, सुरक्षेबाबतच्या पायाभूत सोयींची चाचणी घेतली जावी. बँकांनी त्यांच्या प्रणाली, अधिक चांगली सुरक्षा व नियंत्रण देणा-या, नवनवीन आवृत्त्या वापरुन अद्यावत कराव्यात.

(एन) परिपत्रक डीबीएस.सीओ.आयटीसी.बीसी.10/ 31.09.001/ 97-98 दिनांक 4 फेब्रुवारी 1998/युबीडी क्र.एडीएमएन 46बी/17:36:00/97-98 दिनांक मार्च 30, 1998 अन्वये रिस्क्स अँड कंट्रोल्स इन कॉंप्युटर्स अँड टेलिकम्युनिकेशन्स वर दिलेली मार्गदर्शक तत्वे, आणि माहिती सुरक्षा, इलेक्ट्रॉनिक बँकिंग, तंत्रज्ञान जोखीम व्यवस्थापन व सायबर फसवणुकीवरील कार्यकारी गटाच्या (अध्यक्ष - श्री. जी. गोपालकृष्ण, कार्यकारी संचालक) शिफारशींबाबत (ह्या शिफारशींचे पालन करण्यास बँकांना सांगण्यात आले आहे) परिपत्रक डीबीएस.सीओ आयटीसी.बीसी. क्र.6/31.02.008/2010-11 दिनांक एप्रिल 29, 2011 अन्वये दिलेली मार्गदर्शक तत्वे, इंटरनेट बँकिंगलाही लागु होतील.

(ओ) एसटीसीबी/डीसीसीबींच्या बाबतीत, नाबार्डचे परिपत्रक, एनबी.डीओएस.एचओ.पीओएल क्र. 3634/J-1/2014-15 दिनांक फेब्रुवारी 25, 2015 मधील इंट्रोडक्शन ऑफ आयएस ऑडिट पॉलिसी वरील मार्गदर्शक तत्वेही त्यांना लागु होतील.

(2) वैधानिक प्रश्न

(अ) बँका, त्याच्या ग्राहकाला, त्याने/तिने, खास लेखी किंवा सत्यांकन केलेल्या इलेक्ट्रॉक रीतीने विनंतीच्या आधारावर, सकारात्मक पोच-पावती देऊन इंटरनेट बँकिंग सुविधा देऊ शकतात.

(ब) प्रचलित असलेली कायदेशीर स्थितीचा विचार करता, इंटरनेट बँकिंगचा पर्याय निवडणा-या ग्राहकाबाबत, बँकांचे दायित्व, केवळ त्याची ओळख पटविण्यापुरतेच नव्हे तर, ग्राहकाची सचोटी व पत ह्याबाबत चौकशी करणे हे देखील आहे. ह्यासाठी, खाते उघडण्यासाठी इंटरनेटवर केलेल्या विनंतीचा स्वीकार केला गेला तरीही, त्या ग्राहकाचे खाते, केवायसी निकषांचे पालन करुन, व त्या ग्राहकाच्या ओळखीबाबत पडताळणी करुनच उघडले जावे.

(क) कायद्याच्या दृष्टीने, एखाद्या उपभोक्त्याचे सत्यांकन करण्यासाठी बँकांनी अंगिकारलेली सुरक्षा-कार्यकृती, सहीच्या ऐवजी/बदली म्हणून कायद्याने ओळखले जाणे आवश्यक आहे. माहिती तंत्रज्ञान अधिनियम 2000 च्या तरतुदी व इतर वैधानिक आवश्यकतांचे काटेकोरपणे पालन करणे, इंटरनेट बँकिंग सुविधा देतेवेळी करणे आवश्यक आहे.

(ड) सध्याच्या परिस्थितीत, ग्राहकांची खाती/माहितीची गुप्तता व गोपनीयता ठेवण्याचे दायित्व बँकांवर आहे. इंटरनेट बँकिंगबाबत, वरील दायित्व पुरे न करणा-या बँकांची जोखीम अनेक घटकांमुळे खूप मोठी आहे. शक्य तेवढ्या सर्व काळज्या घेतल्या असल्या तरीही, गुप्ततेचा भंग, सेवा नाकारणे, हॅकिंग/तांत्रिक बिघाड इत्यादींमुळे, बँकांचे ग्राहकांप्रती असलेल्या दायित्वाची जोखीम उच्चतर होऊ शकते. ह्यासाठी, अशा जोखमी हाताळण्यासाठी योग्य असे जोखीम-नियंत्रण उपाय ठेवणे बँकांसाठी आवश्यक आहे.

(3) अंतर्गत नियंत्रण प्रणाली

इंटरनेट बँकिंग देऊ करण्यापूर्वी, बँकांनी सशक्त अशा अंतर्गत नियंत्रण प्रणाली विकसित केल्या पाहिजेत. ह्यामध्ये इंटरनेट बँकिंगशी संबंधित अंतर्गत तपासणी/ऑडिट करावयाच्या प्रणाली, आणि डेटाची एकात्मकता, ग्राहकाची गोपनीयता व डेटाची सुरक्षा ह्यांचे रक्षण करण्यासाठी योग्य ते सुरक्षा उपाय असल्याची खात्री करुन घ्यावी. इंटरनेट बँकिंग मार्फत केलेल्या व्यवहारांवर, ग्राहकांसाठी योग्य अशा आर्थिक मर्यादा विहित करण्याचा विचार बँका करु शकतात. अंतर्गत नियंत्रण प्रणालीमध्ये पुढील गोष्टींचा समावेश असावा.

(अ) भूमिका व जबाबदा-या/संस्थात्मक रचना : अंतर्गत नियंत्रण प्रणाली व्यवस्थितपणे कार्य करत आहे, ह्याची खात्री करुन घेण्याबाबत, संचालक मंडळ व वरिष्ठ व्यवस्थापन जबाबदार असेल. संचालक मंडळाच्या ऑडिट समितीमध्ये, माहिती प्रणाली व संबंधित नियंत्रणे व ऑडिट बाबतचे प्रश्न ह्यांचे पर्याप्त ज्ञान असलेला एक सभासद नेमलेला असावा.

(ब) ऑडिट-धोरणामध्ये आयएस ऑडिटचाही समावेश : बँकांच्या अंतर्गत ऑडिटमध्ये आयएस ऑडिट हा एक महत्वाचा भाग असावा. ऑडिट करण्यासाठी सहाय्य होण्यासाठी, आवश्यक तेव्हा न्यायवैद्यक (फोरेन्सिक) पुरावा म्हणूनही काम करण्यासाठी आणि वाद-निराकरण करण्यासाठी, एक सशक्त ऑडिट मार्गिका तयार असल्याची खात्री करुन देईल अशी एक प्रणाली बँकांनी तयार -करावी.

(क) अहवाल पाठविणे व पाठपुरावा : ह्यामध्ये, प्रत्यक्ष कार्यकारी कर्मचा-यांद्वारा, वरिष्ठ प्राधिकरणांना अहवाल पाठविणे समाविष्ट आहे. सुरक्षा प्रणाली व कार्यरीतींमध्ये कोणताही भंग झाल्यास, तो त्यापेक्षा वरिष्ठ प्राधिकरणाला व ऑडिट समितीला कळविला जाईल. आयएस ऑडिटर्स, ऑडिट-सारांशाचे एक पत्रक तयार करतील, (त्यात, मूळ योजना ते ऑडिटमध्ये आढळून आलेल्या बाबीपर्यंतच्या संपूर्ण ऑडिट प्रक्रियेचे सिंहावलोकन असेल.) आणि ज्याचे ऑडिट केले आहे त्याच्याशी, ह्यावर त्यांना आढळलेल्या बाबींवर चर्चा करतील व त्यांचे प्रतिसाद मिळवतील. ऑडिटमध्ये आढळलेल्या बाबींसंबंधाने अनुपालन करण्यासाठी,

बँकांकडे एक कालबध्द असे पाठपुरावा धोरण असणे आवश्यक आहे. सुरक्षा व कार्यरीतीमधील गंभीर त्रुटींबाबत संचालक मंडळाला कळविणे आवश्यक आहे.

सायबर-सुरक्षेबाबतच्या महत्वाच्या घटना, संचालक मंडळ/वरिष्ठ व्यवस्थापन/आरबीआय/नाबार्ड ह्यांना कळविण्यासाठी/वर नेण्यासाठी, बँकांकडे एक संदेशन योजना असावी.

(4) इतर प्रश्न व प्रकटीकरणे

बँकांवरील विद्यमान विनियामक साचा इंटरनेट बँकिगसाठीही लागु असेल. ह्याबाबत सांगण्यात येते की,

(अ) इंटरनेट बँकिंगखाली असलेले उत्पाद, केवळ खातेदारांपुरतेच सीमित असावेत.

(ब) ह्या सेवांमध्ये केवळ स्थानिक चलनामधील उत्पादच असावेत.

(क) इंटरनेटद्वारा बँकिंग करतेवेळी, ग्राहकांच्या जोखमी, जबाबदा-या व दायित्वे ह्याबाबत, सहकारी बँकांनी प्रकटीकरण करावे.

(ड) इंटरनेट बँकिंग उपलब्ध करतेवेळी, बँकांनी, केवायसीची मार्गदर्शक तत्वे/एएमएल मानके, आणि पीएमएलए 2002 खाली दिलेल्या निदेशांचे व तरतुदींचे पालन करावे.

जोडपत्र - 2

इंटरनेट बँकिंग - सुरक्षा लक्षणे :

(1) सहकारी बँकांनी, त्यांचे वेब ॲप्लिकेशन्ससाठी, सुयोग्य असे सुरक्षा उपाय ठेवले असल्याची खात्री करुन घेणे गरजेचे आहे. तसेच, वेब-सुरक्षेचे निरनिराळे धोके/जोखमी टाळण्यासाठी वाजवी उपाय ठेवणे आवश्यक आहे.

(2) वेबच्या ॲप्लिकेशन्समध्ये, एचटीएमएलच्या गुप्त फाईल्समधील संवेदनशील माहिती, कुकीज्, साठवू नये, किंवा डेटाच्या एकात्मतेमध्ये तडजोड होईल अशी, ग्राहकाच्या बाजूकडील माहिती साठविली जाऊ नये. क्रिटिकल वेब ॲप्लिकेशन्सनी, सर्व ऑनलाईन कार्यकृतींसाठी, किमान एसएसएल व्ही3 किंवा एक्स्टेंडेड व्हॅलिडेशन-एसएसएल/टीएलएस 1.0 128 एनक्रिप्टेशन स्तराची अंमलबजावणी करावी.

(3) एखादे सत्र खंडित केल्यानंतर ते पुनर्स्थापित करण्यासाठी, नॉर्मल युजर ओळख, सत्यांकन व प्राधिकृतता-प्राप्ती घेणे आवश्यक असावे. ह्याशिवाय, स्ट्रॉंग सर्व्हर साईड व्हॅलिडेशन एनेबल केले जावे.

(4) तंत्रज्ञानाच्या वेगवेगळ्या स्तरांवर, सशक्त असे सुरक्षा उपाय वापरुन, सहकारी बँकांनी, खोलवर-सुरक्षा-पवित्रा अनुसरणे गरजेचे आहे.

इंटरनेट बँकिंगसाठी सत्यांकनाच्या रीती

(1) सत्यांकनाच्या रीतींमध्ये तीन मूलभूत घटक असतात.

- युजरला ज्ञात असलेले काहीतरी (उदा. पासवर्ड, पिन)

- युजरजवळ असलेले काहीतरी (उदा. एटीएम कार्ड, स्मार्ट कार्ड) आणि

- युजर स्वतः आहे असे काहीतरी (उदा. बायोमेट्रिक लक्षण-बोटाचा ठसा).

(2) योग्य प्रकारे डिझाईन करुन अंमलात आणलेल्या बहुघटकीय सत्यांकन रीती, अधिक विश्वासार्ह असतात, आणि फसवणुकी टाळण्यास अधिक समर्थ असतात व तडजोड करण्यास अवघड असतात. द्वि-घटक सत्यांकनाचे मुख्य उद्देश म्हणजे, ग्राहकाच्या खात्याची व व्यवहारांची माहिती ह्यांचे संरक्षण करणे, आणि त्याचबरोबर, फिशिंग, की-लॉगिंग, स्पायवेअर/मॅलवेअर ह्यासारख्या निरनिराळ्या सायबर-हल्ला यंत्रणा तसेच बँका व त्यांचे ग्राहक ह्यांच्याबाबत केलेल्या, इंटरनेट आधारित फसवणुकी ह्यांच्याशी यशस्वी सामना करुन, ग्राहकाचा इंटरनेट बँकिंगवरील विश्वास वाढविणे.

इंटरनेट बँकिंगसाठी द्‌वि-घटकीय सत्यांकन व इतर सुरक्षा उपायांची अंमलबजावणी

(ए) सायबर हल्ल्यांचा होणारा प्रसार व त्यांचे भावी परिणाम विचारात घेता, बँकांनी, इंटरनेट बँकिंगमार्फत निधी हस्तांतरणासाठी, द्‌वि-घटकीय सत्यांकनाची अंमलबजावणी करावी.

(बी) सत्यांकनासाठीच्या सुयोग्य रीतींची अंमलबजावणी, त्या संस्थेच्या इंटरनेट बँकिंग प्रणालीबाबत येऊ शकणा-या जोखमींच्या मूल्यमापनावर आधारित असावी. अशा जोखमीचे मूल्यमापन, ग्राहकाचा प्रकार (फुटकळ, कॉर्पोरेट/व्यापारी), ग्राहकाची व्यवहार-क्षमता (उदा. बिल प्रदान, निधी हस्तांतरण), ग्राहकाच्या माहितीची संवेदनशीलता आणि संबंधित व्यवहारांचे आकारमान, विचारात घेऊन केले जावे.

(सी) तंत्रज्ञान-घटकाव्यतिरिक्त एखाद्या सत्यांकन रीतीचे यश, योग्य अशी धोरणे, कार्यरीती व नियंत्रणे ह्यावर अवलंबून असते. एखाद्या परिणामकारक सत्यांकन रीतीच्या बाबतीत पुढील गोष्टी विचारात घेतल्या जाव्यात. ग्राहकाद्‌वारे स्वीकार, वर्धिष्णुता सामावून घेण्याची क्षमता, आणि इतर प्रणालींबरोबरची आंतर-क्रियाशीलता.

(डी) इलेक्ट्रॉनिक व्यवहारांचे सत्यांकन करण्यासाठी, ॲसिमेट्रिक क्रिप्टोसिस्टिम व हॅश फंक्शन न वापरण्यामध्ये एक कायदेशीर जोखीम आहे. निधी हस्तांतरणासारखे विशिष्ट व्यवहार करण्यासाठी, बँकांनी, किमानपक्षी, एक म्हणजे, युजर आयडी/पासवर्ड संयोग, आणि (दुसरा म्हणजे) (अ) डिजिटल सही (डिजिटल प्रमाणपत्र व त्याला संलग्न खाजगी की असलेल्या टोकन मार्फत (विशेषतः कॉर्पोरेट ग्राहकांसाठी) किंवा (ब) वन टाईम पासवर्ड (ओटीपी)/निरनिराळ्या रितींमार्फत (मोबाईल फोनवरील एसएमएस, किंवा हार्डवेअर टोकन) दिलेला डायनॅमिक ॲक्सेस, असे सशक्त व गतिशील द्‌वि-घटकीय सत्यांकन अंमलात आणू शकतात.

(ई) ऑनलाईन प्रक्रियेची सुरक्षा वाढविण्यासाठी, पूर्व नियोजित मूल्यापेक्षा अधिक मूल्याच्या व्यवहारांसाठी, नवीन अकाऊंट लिंकेजेस् निर्माण करण्यासाठी, तृतीय पक्ष आदेशितीच्या वेळी तपशीलाचे पंजीकरण करण्यासाठी, खात्याचा तपशील बदलण्यासाठी, किंवा निधी हस्तांतरणाच्या मर्यादा बदलण्यासाठी, दुजोरा देणा-या, सेकंड चॅनल कार्यरीती (जसे, टेलिफोन, एसएमएस, ई-मेल इत्यादि) वापरल्या जाव्यात अशी सुरक्षा लक्षणे तयार करताना, बँकांनी, त्या लक्षणांची परिणामकारकता व अतिरिक्त ऑनलाईन सुरक्षेसाठी ग्राहकांची पसंतीही विचारात घ्यावी.

(एफ) उभयपक्षी संमत सत्यांकन व्यवहार-संहितेवर आधारित, ग्राहकही, बँकेच्या वेबसाईटचे सत्यांकन, सुरक्षा यंत्रणाद्‌वारे करु शकतात. जसे - वैय्यक्तिक/वचन-संदेश/प्रतिमा, चॅलेंज रिस्पॉन्स सुरक्षा संकेतांची देवाण-घेवाण, आणि/किंवा सिक्युअर सॉकेट्स लेयर (एसएसएल) सर्व्हर प्रमाणपत्राचे सत्यांकन, अलिकडील काळात, एक्स्टेंडेड व्हॅलिडेशन सिक्युअर सॉकेट्स लेयर (ईव्ही-एसएसएल) प्रमाणपत्रांचा वापर मोठ्या प्रमाणावर केला

जात आहे. ही खास अशी एसएसएल प्रमाणपत्रे असून, एखाद्या वेबसाईटची संस्थात्मक ओळख स्पष्टपणे करुन देण्यास, उच्च सुरक्षा वेब ब्राउझर्ससह काम करतात. तथापि, येथे नोंद घेतली जावी की, एसएसएल हे केवळ, नेटवर्कच्या ट्रान्सपोर्ट लेयरवर इन ट्रान्झिट असलेला डेटा एनक्रिप्ट करण्यासाठी तयार करण्यात आले आहे. ते, ॲप्लिकेशन लेयरवर, एंड-टु-एंड एनक्रिप्टेशन सुरक्षा उपलब्ध करुन देत नाही.

(जी) सत्यांकन केलेले एखादे सत्र, तिच्या एनक्रिप्टेशन प्रोटोकॉलसह, ग्राहकाशी केलेल्या दळणवळणामध्ये संपूर्णपणे अखंडित असावे अन्यथा, त्यात व्यत्यय आल्यास ते बंद केले जावे व त्यामुळे बाधित झालेले व्यवहार, निश्चित (रिझॉल्स्) केले जावेत किंवा रिव्हर्स केले जावेत. असे सत्र समाप्त होत असताना, अशा घटनेबाबत ग्राहकाला ताबडतोब कळविण्यात यावे किंवा त्यानंतर ई-मेल, फोन किंवा इतर साधनांनी कळविले जावे.

(एच) मोबाईल फोन नंबरमधील बदल हा केवळ शाखेमार्फत केलेल्या विनंतीमार्फतच केला जावा.

(आय) व्हेच्युअल की बोर्ड स्थापन करावा.

(जे) नवीन लाभार्थी समाविष्ट केल्यास, अशा लाभार्थींना समाविष्ट करण्यासाठी एक कूलिंग कालावधी ठेवावा आणि एसएमएस/ई-मेल द्वारे इशारे दिले जावेत.

(के) ग्राहकांना, त्यांचा पर्सनल कॉम्प्युटर्सचे रक्षण करण्यासाठी असलेल्या निरनिराळ्या सुरक्षा काळज्या घेण्यासाठी, आणि त्यांचे आर्थिक व्यवहार, सार्वजनिक किंवा इंटरनेट कॅफेमधील कॉम्प्युटर्समधून करणे टाळण्यास सांगितले जावे.

(एल) एक आनुषंगिक बाब म्हणून, जोखीम-आधारित व्यवहार देखरेख किंवा देखरेख प्रक्रियेचा विचार करण्याची गरज आहे.

(एम) विद्यमान सत्र चालु ठेवण्यासाठी ग्राहकाचे पुनर्-सत्यांकन करावयाचे नसल्यास, ऑन-लाईन सत्र, एका ठरीव कालावधीनंतर आपोआप बंद होणे गरजेचे आहे. ह्या मुळे आक्रमण करणाराला इंटरनेटचे सत्र अनिश्चित कालासाठी सुरु ठेवण्यास प्रतिबंध होतो.

(एन) केलेल्या व्याख्येनुसार, बहु-घटकीय सत्यांकन करण्यासाठी, घटकांच्या तीन प्रकारांपैकी दोन किंवा अधिक घटकांमधील सोल्युशन्सची आवश्यकता असते. त्याच घटक प्रकारामधील अनेक सोल्युशन्स, त्या प्रक्रियेमधील निरनिराळ्या ठिकाणी वापरणे हे, लेयर्ड सुरक्षेचा किंवा अन्य कॉपेन्सेटिंग कंट्रोल ॲप्रोचचा भाग असू शकते. परंतु, ख-या अर्थाने ते, बहु-घटकीय सत्यांकन असणार नाही.

(ओ) द्वि-घटकीय सत्यांकन रचनेचा एक महत्वाचा भाग म्हणून, बँकांनी, मध्यस्थ लोकांनी केलेला हल्ला (ह्याला मॅन-इन-दि-मिडल ॲटॅक (एमआयटीएम), मॅन-इन-दि-ब्राउझर (एमआयटीबी) ॲटॅक किंवा मॅन इन

दि ॲप्लिकेशन ॲटॅक असेही म्हटले जाते) होण्याबाबतचा धोका किमान करण्यासाठी सुयोग्य उपाय योजावेत.

(पी) मॅन इन दि मिडल ॲटॅक्स किमान करण्यासाठी, बँकांनी, त्यांना योग्य वाटल्यास, पुढील नियंत्रण व सुरक्षा उपाय करण्याचा उपाय करावेत.

(1) **नवीन आदेशिती (पेयीज्) समाविष्ट करण्यासाठी विशिष्ट ओटीपीज्** :- प्रत्येक नवीन आदेशितीला, दुस-या एका चॅनलकडील (ज्यात आदेशितीचा तपशील दिला असेल अशा किंवा बँकेद्वारा पडताळणी केल्या गेलेल्या व व्यक्तिशः (मॅन्युअल) कार्यरीतींनुसार मिळालेल्या, ग्राहकाने स्वहस्ते केलेल्या सही वर) ओटीसीवर आधारित, ग्राहकाने प्राधिकृत करावे.

(2) **मूल्याधारित व्यवहारांसाठी (प्रदाने व निधी हस्तांतरणे) वैय्यक्तिक ओटीपी** :- मूल्याधारित प्रत्येक व्यवहारासाठी किंवा ग्राहकाने ठरविलेल्या विशिष्ट आर्थिक मर्यादेबाहेरील, मंजुरीप्राप्त यादीमधील मूल्याधारित व्यवहारांसाठी एक नवा ओटीपी लागेल.

(3) **ओटीपी टाईम विंडो** :- आव्हान-आधारित व समय आधारित ओटीपीज् भक्कम सुरक्षा देतात, कारण त्यांचा परिपक्वता काल संपूर्णतः बँकेद्वारा नियंत्रित केला जातो आणि तो युजर बिहेवियरवर अवलंबून असत नाही. ह्यासाठी शिफारस करण्यात येते की, बँकांनी, ओटीपी टाईम विंडो, सर्व्हर टाईमच्या दोन्हीही बाजूस 100 सेकंदापेक्षा जास्त ठेवू नये. कारण, टाईम विंडो जेवढी छोटी असेल, तेवढीच ओटीपीच्या गैरवापरांची जोखीमही कमी असते.

(4) **प्रदान व निधी हस्तांतरण सुरक्षा** :- मध्यस्थ व्यक्तीने केलेल्या हल्ल्यामध्ये (मिडल मॅन ॲटॅक) बदल करणे किंवा हस्तांतरणाच्या डेटामध्ये घुसवणे/घुसखोरी करणे, शोधण्यासाठी, निधी हस्तांतरण व्यवहारांसाठी, डिजिटल सह्या व की-बेस्ड मेसेज ऑथेंटिकेशन कोड्स (केएमएसी) ह्यांचा विचार केला जाऊ शकतो. हा सुरक्षा उपाय परिणामकारकतेने कार्यशील होण्यासाठी, हार्डवेअर टोकन वापरणा-या ग्राहकाने, एखाद्या व्यवहारात डिजिटल सही करण्याच्या प्रक्रियेमधून, एक वन टाईम पासवर्ड निर्माण करण्याची प्रक्रिया ओळखण्यास सक्षम असणे आवश्यक आहे. त्याने डिजिट स्वरुपात सही केली त्याचा अर्थ त्याला कळला पाहिजे, ह्याचाच अर्थ, डिजिटल सही निर्माण करण्यासाठी ज्याच्यामधून हॅश व्हॅल्यु काढता येईल अशा प्रकारे खाते क्रमांक व प्रदानाची रक्कम, त्या टोकनने स्पष्टपणे/नेमकी दर्शविली पाहिजे. ओटीपी निर्माण करण्यासाठी व व्यवहारांवर सही करण्यासाठी निरनिराळ्या क्रिप्टो कीज्चा वापर केला जावा.

(5) इंटरनेट बँकिंगच्या परिस्थितीत, ग्राहकांद्वारा दिल्या जाणा-या स्टॉप-पेमेंट सूचनांवर कारवाई करण्यास बँकांना अत्यल्प वाव आहे. ह्यासाठी, बँकांनी, स्टॉप पेमेंटच्या सूचना स्वीकारण्यासाठीची परिस्थिती व कालावधी त्यांना ग्राहकांना अधिसूचित करावा.

(6) ग्राहक संरक्षण अधिनियम 1986 मध्ये, भारतातील उपभोक्त्यांच्या हक्कांची व्याख्या करण्यात आली असून, ती बँकिंग सेवांनाही लागु आहे. इंटरनेट बँकिंगचा लाभ घेणा-या ग्राहकांचे हक्क व दायित्वे, इंटरनेट बँकिंगचा पर्याय निवडणा-या ग्राहकांना स्पष्टपणे समजावून सांगण्याची गरज आहे. बँकिंगचा व्यवसाय आणि पारंपरिक बँकिंगमधील ग्राहकांनी त्याबाबतच्या हक्कांचा घेतलेला लाभ विचारात घेता, हॅकिंग केले गेल्यामुळे झालेले अनधिकृत हस्तांतरण, तांत्रिक बिघाडामुळे सेवा न दिली जाणे, इत्यादींमुळे बँकांचे ग्राहकांसाठीचे दायित्व ह्यांचे पुनर्मूल्यांकन केले जाणे आवश्यक आहे, आणि इंटरनेट बँकिंग देऊ करणा-या बँकांनी, अशा जोखमींविरुध्द विमासंरक्षण घ्यावयास हवे.

(7) बँकांच्या हायपरलिंक्समुळे अनेकदा नावलौकिकात्मक धोके/जोखमीने प्रश्न निर्माण होतात. अशा लिक्संमुळे, बँकेशी संबंध नसलेला कोणताही उत्पाद किंवा व्यवसाय त्या बँकेद्वारे प्रायोजित करण्यात येत आहे अशी ग्राहकाची दिशाभूल केली जाऊ नये. बँकेच्या हायपरलिंक्स वेबसाईटमधील त्या बँकांची ज्यांच्याबरोबर प्रदान व्यवस्था आहे अशाच पोर्टल्सपुरती सीमित असावी. इतर पोर्टल्सकडून बँकेच्या वेबसाईटशी असलेल्या हायपर लिंक्स ह्या, सर्वसामान्यतः, बँकेच्या ग्राहकांनी त्या पोर्टलमध्ये केलेल्या खरेदी संबंधीची माहिती प्रसारित करण्यासाठी असतात. ग्राहकांच्या खरेदीसंबंधाने, इतर वेबसाईट्सकडून आलेल्या विनंत्या हाताळतांना, बँकांनी, शिफारस केलेल्या सुरक्षा-सावधानता पाळणे अत्यावश्यक आहे.

(8) **दुस-या वाहिनीमार्फत अधिसूचना/दुजोरा** :- ग्राहकाने ठरविलेल्या विशिष्ट मूल्यापेक्षा अधिक झालेली सर्व प्रदाने किंवा निधी हस्तांतरणे, बँकेने ग्राहकाला एका दुस-या वाहिनीमार्फत अधिसूचित करावीत.

(9) **एसएसएल सर्व्हर प्रमाणपत्र इशारा** :- एसएसएल् किंवा ईव्ही-एसएसएल प्रमाणपत्र इशा-याला कसा प्रतिसाद द्यावा ह्याची इंटरनेट बँकिंग ग्राहकांना जाणीव करुन द्यावी व दाखविलेही जावे.

(10) बँकांनी, जोखीम आधारित व्यवहार देखरेख व नजर ठेवण्याची प्रक्रिया ठेवावी. अशा सॉफ्टवेअरमध्ये, ग्राहकाच्या व्यावहारिक वर्तणुकीचा साचा, अनियमित व्यवहार थांबविणे, किंवा मर्यादेबाहेरील व्यवहारांबाबत ग्राहकाचा पूर्व-दुजोरा घेणे ह्यांचाही समावेश केला जावा.