భారతీయ రిజర్వ్ బ్యాంక్

www.rbi.org.in

RBI/2015-16/229 November 05, 2015

DCBR.BPD. (PCB/RCB) Cir.No.6/19.51.026/2015-16

ది చీఫ్ ఎక్జిక్యూటివ్ ఆఫీసర్

అన్ని ప్రాథమిక (పట్టణ) సహకార బ్యాంకులు/

రాష్ట్ర మరియు కేంద్ర సహకార బ్యాంకులు

అమ్మా/అయ్యా,

సహకార బ్యాంకుల ఖాతాదార్లకు అంతర్జాల బ్యాంకింగ్ సదుపాయం (ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయం - Internet Banking Facility)

భారతీయ రిజర్వ్ బ్యాంక్, కొన్ని ప్రమాణాలను నెరవేర్చిన, తమ ముందస్తు అనుమతి పొందిన షెడ్యూల్డ్ పట్టణ సహకార బ్యాంకులకు, తమ అంగీకారంపొంది, ఖాతాదార్లకు లావాదేవీలు జరపగలిగే ఇంటర్‌నెట్ బ్యాంకింగ్ సదుపాయం (Internet Banking with Transactional Facility) అందించడానికి, అనుమతినిచ్చింది. (దయచేసి మా సర్క్యులర్ UBD.BPD.(SCB). Cir.No.1/09.18.300/2011-12 తేదీ సెప్టెంబర్ 26, 2011 చూడండి).

అలాగే, అన్ని పట్టణ సహకార బ్యాంకులకు (కొన్ని నిబంధనలు పాటిస్తున్న), వారి ఖాతాదార్లకు ఇంటర్నెట్ బ్యాంకింగ్ (చూచుటకు మాత్రమే) సదుపాయం (Internet Banking (view only) Facility), రిజర్వ్ బ్యాంక్ అంగీకారం పొందనవసరం లేకుండానే, అందించడానికి సమ్మతించింది. (దయచేసి మా సర్క్యులర్ UBD.BPD.(PCB).Cir.No.21/09.18.300/2014-15 తేదీ అక్టోబర్ 13, 2014 చూడండి)

2. స్టేట్ కో-ఆపరేటివ్ బ్యాంకులు (ఎస్ సి బి లు, STCB s), జిల్లా కో-ఆపరేటివ్ బ్యాంకులు (డి సి బి లు, DCB s) ఇంతవరకు వారి ఖాతాదార్లకు, ఇంటర్నెట్ బ్యాకింగ్ సదుపాయం అందించడానికి అనుమతించబడలేదు. అయితే కొన్ని ఎస్ సి బి లు, డి సి బి లు, ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయాలు అందించడానికి అనుమతి కోరడం వల్ల, వారిని కూడా అనుమతించాలని నిర్ణయించడం జరిగింది. తదనుసారంగా, యు సి బి లకు జారీ చేసిన ఆదేశాలు పునఃస్సమీక్షించి, వాటిని అధిగమిస్తూ, అన్ని సహకార బ్యాంకులకు సమానంగా వర్తించేలా మార్గదర్శకాలు జారీ చేయాలని నిర్ణయించడం జరిగింది. సవరించిన మార్గదర్శకాలు ఈ క్రింద ఇవ్వబడ్డాయి:

(i) ఇంటర్నెట్ బ్యాంకింగ్ (చూచుటకు మాత్రమే) సదుపాయం (Internet Banking (view only) Facility)

3. కోర్ బ్యాంకింగ్ సొల్యూషన్స్ (CBS) అమలుపరచిన అన్ని ఎస్ సి బి లు, డి సి సి బి లు మరియు యు సి బి లు, ఇంటర్నెట్ ప్రోటోకాల్ వెర్షన్ 6 (IPv6) కు మారి, అనుబంధం–I లో ఇచ్చిన మార్గదర్శకాలను అనుసరిస్తున్నట్లయితే, ముందుగా రిజర్వ్ బ్యాంక్ ముందస్తు అనుమతి లేకుండానే, వారి ఖాతాదార్లకు ఇంటర్నెట్ బ్యాంకింగ్ (చూచుటకు మాత్రమే) సదుపాయాన్ని అందించవచ్చు. ఏదేని సేవకు రెండు అంచెల ధృవీకరణ అవసరమైనా, లేక వన్ టైమ్ పాస్‌వర్డ్ అవసరమైనా, బ్యాంకులు, అనుబంధం II లో పేర్కొన్న భద్రతా అంశాలు పాటించాలి.

4. బ్యాంకులు, ఈ సదుపాయం కేవలం బ్యాలన్స్ తెలుసుకొనుట, బ్యాలన్స్ చూచుట, అకౌంట్ స్టేట్‌మెంట్ డౌన్‌లోడ్ చేసుకొనుట, చెక్ బుక్ జారీకై వినతిచేయుట వంటి, నగదు లావాదేవీలు లేని సేవలకు మాత్రమే వినియోగపడేలా శ్రద్ధ తీసుకోవాలి. నగదు లావాదేవీలు ఎట్టి పరిస్థితిల్లోనూ అనుమతించరాదు.

5. సహకార బ్యాంకులు, ఇంటర్నెట్ బ్యాంకింగ్ (చూచుటకు మాత్రమే) సేవలు ఆచరణలోకి తెచ్చిన నెల రోజుల లోపు, వారికి సంబంధించిన ప్రాంతీయ రిజర్వ్ బ్యాంక్ కార్యాలయానికి (ఎస్ సి బి లు, డి సి సి బి లు అయితే NABARD కు కూడా) తెలియజేయాలి.

(II) నగదు లావాదేవీలతో సహా ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయం (Internet Banking with Transactional Facility)

6. కోర్ బ్యాంకింగ్ సొల్యూషన్స్ (CBS) అమలుపరచిన, లైసెన్స్ గల, అన్ని ఎస్ సి బి లు, డి సి సి బి లు మరియు యు సి బి లు, ఇంటర్నెట్ ప్రోటోకాల్ వెర్షన్ 6 (IPv6) కు మారి, ఈ క్రింద పేర్కొన్న ప్రమాణాలను నెరవేరుస్తున్నట్లయితే, **రిజర్వ్ బ్యాంక్ ముందస్తు అనుమతితో,** వారి ఖాతాదార్లకు లావాదేవీలతో సహా ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయాన్ని అందించవచ్చు.

a) CRAR 10% కన్న తక్కువ ఉండరాదు.
b) గడిచిన ఆర్థిక సంవత్సరం మార్చ్ 31 న, నికర సంపద రూ. 50 కోట్లు లేదా అంతకు మించి ఉండాలి.
c) మొత్తం నిరర్థక ఆస్తులు (Gross NPAs) 7% కంటె తక్కువ ఉండాలి. నికర నిరర్థక ఆస్తులు (Net NPAs) 3% మించి ఉండరాదు.
d) గడిచిన ఆర్థిక సంవత్సరంలో, నికర లాభం గడించి ఉండాలి. ఇంతేగాక, మొత్తం మీద, ముందటి నాలుగు ఆర్థిక సంవత్సరాలలో, మూడు సంవత్సరాలు, నికర లాభం సంపాదించి ఉండాలి.
e) గడిచిన ఆర్థిక సంవత్సరంలో, CRR/SLR నిర్వహణలో వైఫల్యాలు ఉండరాదు.

f) పటిష్ఠమైన అంతర్గత నియంత్రణ వ్యవస్థ (internal control system) కలిగి ఉండాలి. బోర్డ్ లో కనీసం ఇద్దరు నిపుణులైన డైరెక్టర్లు ఉండాలి.

g) నిబంధనల అనుసరణలో వైఫల్యాలు ఉండరాదు. దరఖాస్తు చేసే సంవత్సరానికి ముందు గడిచిన రెండు ఆర్థిక సంవత్సరాల్లో, రిజర్వ్ బ్యాంక్ నిర్దేశాల /మార్గదర్శకాల ఉల్లంఘనకు జరిమానా విధింపబడి ఉండకూడదు.

7. పై ప్రమాణాలను నెరవేర్చి, అనుబంధం I, II లలో సూచించిన మార్గదర్శకాలను పాటించే ఎస్ సి బి లు, డి సి సి బి లు, యు సి బిలు, లావాదేవీలతో సహా ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయాన్ని అందించడా నికి అనుమతించబడతాయి. ఇందుకై, ఎస్ సి బి లు, డి సి సి బి లు, యు సి బి లు, ఈ క్రింద సూచించిన ప్రమాణ పత్రాలతో, రిజర్వ్ బ్యాంక్ ప్రాంతీయ కార్యాలయానికి (ఎస్ సి బిలు, డి సి సి బి లు, NABARD ద్వారా), దరఖాస్తు చేయాలి.

(i) బోర్డ్ అంగీకరించిన, ఇంటర్నెట్ బ్యాంకింగ్ విధానపు నకలు తోబాటు, ఆర్ బి ఐ మార్గదర్శకాల్లో సూచించిన ఐ టి (IT), ఐ ఎస్ (IS) విధానాలు పాటించబడుతున్నాయని, ఒక స్వతంత్ర ఆడిటర్ (అర్హతగల CISA) నుంచి దృవీకరణ పత్రం.

(ii) అందించే సేవల్లో/ప్రోడక్ట్స్ లో ఏవైన మార్పులు ఉంటే, ఆర్ బి ఐ కి తెలియపరుస్తామని హామీ పత్రం.

(iii) వ్యాపార ప్రణాళిక, వ్యయ/లాభాల విశ్లేషణ, సాంకేతికత, వ్యాపార భాగస్వాములు, పరాయి సేవలు, సంభవి౦చగల నష్టాల నుంచి రక్షణకు, బ్యాంక్ అనుసరించబోయే విధానాలు/ప్రక్రియలు.

8. భద్రతావ్యవస్థలో ఎటువంటి భంగం, వైఫల్యం వాటిల్లినా ఆర్ బి ఐ ప్రాంతీయ కార్యాలయానికి (ఏస్ సి బి/డిసి సి బి లు NABARD కు కూడా) తెలియపరచాలి. రిజర్వ్ బ్యాంక్, అవసరమనిభావిస్తే, ప్రత్యేకమైన ఆడిట్ /తనిఖీని ఆదేశించవచ్చును.

9. ఇదివరకే ఖాతాదార్లకు ఇంటర్నెట్ (చూచుటకు మాత్రమే) బ్యాకింగ్ సదుపాయాల్ని అందిస్తున్న ఎస్ సి బి/డి సి బి లు, తక్షణం ఈ మార్గదర్శకాలననుసరించి వారి విధానాలని సమీక్షించి, ఈ సర్క్యులర్ జారీ చేసిన తేదీ నుండి నెల లోగా, వారందించే సేవలు, మార్గదర్శకాల అమలు గురించిన వివరాలతో, ప్రాంతీయ రిజర్వ్ బ్యాంక్ కార్యాలయానికి (NABARD ద్వారా) నివేదిక పంపాలి. వ్యత్యాసాలు ఉంటే తెలియపరచి, వాటిని సరిదిద్దడానికి తీసుకోబోయే, కాలబద్ధమైన కార్యాచరణ ప్రణాళికని వివరించాలి.

10. ఇదివరకే, లావాదేవీలతోసహా ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయాలు అందిస్తున్న ఎస్ సి బి/డి సి సి బి లు ఈ మార్గదర్శకాలు పాటించాలని సూచించడమైనది. వారి వ్యాపార ప్రణాళిక, వ్యయ/లాభాలపై అంచనా, మొదలైన వివరాలు తెలిపి, ఈ సర్క్యులర్ జారీచేసిన తేదీ నుండి ఒక నెలలోగా రిజర్వ్ బ్యాంక్ 'పోస్ట్ ఫాక్టో' అనుమతి పొందాలి. ఇందులకై అభ్యర్థనలు, రిజర్వ్ బ్యాంక్ ప్రాంతీయ కార్యాలయానికి, NABARD ద్వారా పంపాలి.

విధేయులు,

(సుమా వర్మ)

ప్రిన్సిపల్ చీఫ్ జనరల్ మేనేజర్

జతపరచినవి: పైన తెలిపినవి

అనుబంధం - I

సహకార బ్యాంకుల ఖాతాదార్లకు ఇంటర్నెట్ బ్యాంకింగ్ సౌకర్యంపై మార్గదర్శకాలు

ఖాతాదార్లకు ఇంటర్నెట్ బ్యాంకింగ్ సౌకర్యాన్ని అందించగోరుతున్న, లైసెన్స్ గల, ఎస్ సి బి/ డిసి సి బి/ యుసి బి లు ఈ క్రింది సూచనలు పాటించాలి:

(i) ఇంటర్నెట్ బ్యాంకింగ్ విధానాన్ని, బోర్డ్ అనుమతితో రూపొందించాలి.

(ii) ఈ విధానం, వారి ఇన్ఫర్మేషన్ టెక్నాలజీ, భద్రతా విధానాలకు అనుగుణంగా ఉండి, రికార్డుల గోప్యతనీ, భద్రతనీ కాపాడేట్లుగా ఉండాలి.

(iii) 'మీ వినియోగదారుని తెలుసుకోండి' నిబంధనలని అమలుచేసేందుకు, స్పష్టమైన విధానం కలిగి ఉండాలి.

(iv) సాంకేతిక, భద్రతా ప్రమాణలు పాటించడంతోబాటుబాటు, అనుబంధం లో సూచించిన, చట్ట పరమైన /నియంత్రణ/ పర్యవేక్షణ అంశాలని కూడా పరిగణనలోకి తీసుకోవాలి.

(v) బ్యాంకులు, పటిష్ఠమైన అంతర్గత నియంత్రణా వ్యవస్థ కలిగి ఉండి, ఈ సేవలందించడంలో కలుగబోయే నష్టాలని దృష్టిలో ఉంచుకోవాలి.

(vi) ఖాతాదార్లకు, ఈ సదుపాయంలో ఉన్న ప్రమాదాలనీ, కర్తవ్య బాధ్యతలనీ, ముందే తెలియచెయ్యాలి.

తదనుగుణంగా, ఆచరణకై బ్యాంకులకు ఈ క్రింది మార్గదర్శకాలు జారీ చేయబడ్డాయి.

I. సాంకేతిక, భద్రతా ప్రమాణాలు:

a. సహకార బ్యాంకులు, బోర్డ్ ఆఫ్ డైరెక్టర్లు అమోదించిన ఇన్ఫర్మేషన్ టెక్నాలజీ భద్రతా విధానం కలిగి ఉండాలి. ఇన్ఫర్మేషన్ టెక్నాలజీ (ఐ టి) మరియు ఇన్ఫర్మేషన్ భద్రతా (ఐ ఎస్) విభాగాల మధ్య విధుల వితరణ స్పష్టంగా ఉండాలి. ఐ టి విభాగం కంప్యూటర్ సిస్టమ్ లను నిర్వహిస్తుంది. ఇన్ఫర్మేషన్ సెక్యూరిటీ అధికారి, ఇన్ఫర్మేషన్ భద్రతా

అంశాలు అమలు పరచాలి. ఇంతేగాక, ఇన్ఫర్మేషన్ సిస్టమ్స్ ఆడిటర్, ఇన్ఫర్మేషన్ సిస్టమ్స్‌ని ఆడిట్ చెయ్యాలి.

b. బోర్డ్ అనుమతితో, బ్యాంకులు ఐ ఎస్ విధానానికి అనుగుణంగా విధుల నిర్వహణకు, ఒక నెట్ వర్క్ అండ్ డాటాబేస్ అడ్మినిస్ట్రేటర్ ని (Network and Database Administrator) నియమించాలి.

c. డాటా, సిస్టమ్స్, అప్లికేషన్ సాఫ్ట్‌వేర్, యుటిలిటీస్, టెలికమ్యూనికేషన్ లైన్స్ , లైబ్రరీస్, సిస్టమ్ సాఫ్ట్‌వేర్ మొదలైన వాటి లాజికల్ ఏక్సెస్ (logical access) కు తగిన నియంత్రణలు అమలులో ఉండాలి.

d. ఇంటర్నెట్ కు, బ్యాంక్ సిస్టమ్ కు మధ్య నేరుగా సంబంధం ఉండరాదు.

e. సిస్టమ్/నెట్‌వర్క్ లోకి చొరబాటులు (intrusions) నివారించడానికి కట్టుదిట్టమైన రక్షణ వ్యవస్థ ఉండాలి.

f. అప్లికేషన్ సర్వర్ లో, ఫైల్ ట్రాన్స్ఫర్ ప్రోటోకాల్ (FTP), టెల్‌నెట్ వంటి నిరుపయోగమైన సేవల్ని నిర్వీర్యం (disable) చేయవలెను. అప్లికేషన్ సర్వర్ ని, ఇ-మైల్ సర్వర్ నుండి వేరుచేయవలెను.

g. కంప్యూటర్ ఏక్సెస్‌లు అన్నిటినీ 'లాగ్' చేసి, జరిగిన/జరపబోయిన భద్రతా ఉల్లంఘనలని రికార్డ్ చేసి తదుపరి చర్యలను చేపట్టవలెను. సిస్టమ్స్, నెట్‌వర్క్‌లపై చొరబాటులను, దాడులను అరికట్టేందుకు తగిన సాధనాలను సమకూర్చుకొని, వీటిని నిరోధించవలెను. బ్యాంకులు, భద్రతా వ్యవస్థని/విధానాలని నిరంతరం సమీక్షిస్తూ, వారి అనుభవాలని, మారుతున్న సాంకేతికతను దృష్టిలో ఉంచుకొని, మెరుగు పరుచుకోవాలి.

h. ఇన్ఫర్మేషన్ సెక్యూరిటీ ఆఫీసర్, ఇన్ఫర్మేషన్ ఆడిట్ ఆఫీసర్, నిర్ణీత కాల వ్యవధుల్లో ఈ క్రింద పేర్కొన్న 'పెనెట్రేషన్ టెస్టులు' (penetration tests) నిర్వహించవలెను:

1. పాస్‌వర్డ్ క్రాకింగ్ టూల్స్ (password cracking tools) ఉపయోగించి పాస్‌వర్డ్ తెలుసుకొనుట
2. ప్రోగ్రామ్ లో 'బ్యాక్ డోర్ ట్రాప్స్' వెదకుట
3. Distributed Denial of Service (DDOS), denial of Service (DoS) అటాక్స్ ఉపయోగించి, సిస్టమ్ ని ఓవర్‌లోడ్ చేయుటకు ప్రయత్నించుట
4. బ్రౌజర్, ఇ-మైల్ సాఫ్ట్‌వేర్ ఉంటే, సాఫ్ట్‌వేర్ లో, సామాన్యంగా ఉండే లొసుగులు వెదకుట
5. పెనెట్రేషన్ టెస్టింగ్, ఎతికల్ హ్యాకర్స్ (ethical hackers) అని పిలువబడే, బయటి నిపుణుల ద్వారాకూడా చేయించవచ్చు.

i. ఇన్‌ఫర్‌మేషన్ సిస్టంలు, సైట్ లు ఎక్కడ ఉన్నా, లోపలి, బయటి ప్రమాదాలనుంచి కాపాడడానికి, ఫిజికల్ ఏక్సెస్ నియంత్రణలు (Physical Access Controls) ఖచ్చితంగా అమలుపరచాలి.

j. బ్యాంకులు, డాటా బాక్ అప్ (data back-up) చేయడానికి తగిన వ్యవస్థ, కాల పట్టిక (schedule) కలిగి ఉండాలి. బాక్ అప్ డాటానుండి, లావాదేవీల వివరాలు నష్టపోకుండా, తిరిగి పొందగలమా అని. బ్యాంక్ భద్రతా విధానం ప్రకారం నిర్ణయించిన కాల అవధుల్లో, పరీక్షిస్తూ ఉండాలి.

k. చట్ట పరమైన అవసరాల కోసం, అన్ని దరఖాస్తుల రికార్డ్ ఉండాలి. అందుకొన్న/పంపబడిన మెసేజ్‌ల రికార్డ్ ఎన్‌క్రిప్టెడ్/డిక్రిప్టెడ్ రీతిలో భద్రపరచాలి.

l. ఇంటర్‌నెట్ బ్యాంకింగ్ సాఫ్ట్‌వేర్ అమలుచేసే ముందు బ్యాంకులు, విక్రేత నుండి, 'అప్లికేషన్ ఇంటెగ్రిటీ స్టేట్‌మెంట్' తీసుకొని తీరాలి.

m. సిస్టం లు, సాధారణ అప్లికేషన్ లు ఉపయోగించేముందు, భద్రతా వ్యవస్థను పరీక్షించాలి. మెరుగైన భద్రత, నియంత్రణ కోసం కాలానుసారంగా, సిస్టంలను పైశ్రేణికి మార్చుకోవాలి

n. 'ఇన్ఫర్మేషన్ సెక్యూరిటీ, ఎలెక్ట్రానిక్ బ్యాంకింగ్, టెక్నాలజీ రిస్క్ మేనేజ్మెంట్ మరియు సైబర్ ఫ్రాడ్స్' పై కార్య నిర్వాహక వర్గం (ఛైర్మన్ : శ్రీ జి. గోపాల కృష్ణ) చేసిన సిఫారసుల దృష్ట్యా, రిజర్వ్ బ్యాంక్ జారీ చేసిన 'రిస్క్స్ అండ్ కంట్రోల్స్ ఇన్ కంప్యూటర్స్ అండ్ టెలికమ్యూనికేషన్స్' (DBS.CO.ITC.BC.10/31.09.001/97-98, dated 4th February 1998; UBDNo.Admn.46b/17:36:00/97-98, dated March 30, 1998 and circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011) లోని మార్గదర్శకాలు, ఇంటర్నెట్ బ్యాంకింగ్ సేవలకి కూడా సమానంగా వర్తిస్తాయి.

o. ఎస్ సి బి/డి సి సి బి ల విషయంలో, NABARD సర్క్యులర్లో (NB.DoS.HO.POL.No.3634/J-1/2014-15, February 25, 2015) గల మార్గదర్శకాలు కూడా వర్తిస్తాయి.

II. చట్టపరమైన విషయాలు

a. బ్యాంకులు, ఖాతాదార్లకు ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయాన్ని, వారు లిఖితపూర్వకంగా లేదా ప్రమాణీకృత (authenticated) ఎలక్ట్రానిక్ అభ్యర్థన ద్వారా కోరితేనె అందించాలి

b. ప్రస్తుతం ఉన్న చట్టాల ప్రకారం, ఖాతాదారు యొక్క గుర్తింపేగాక, అతని నిజాయితీ, పేరు ప్రతిష్ఠల గురించి కూడా వాకబు చేయాల్సిన బాధ్యత బ్యాంకులపై ఉంది. అందువల్ల , ఇంటర్నెట్ ద్వారా వచ్చిన దరఖాస్తును అంగీకరించినా, KYC నిబంధనలు పాటించిన తరువాతే ఖాతాలు తెరవాలి.

c. ఖాతాదారుని ధ్రువ పరచుకోవడానికి, బ్యాంకులు ఆచరించే భద్రతావిధానం, చట్టపరంగా, సంతకానికి బదులుగా పనికివస్తుంది అని, గుర్తించబడాలి. అందువల్ల, ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయం అందించేముందు, ఇన్ఫర్మేషన్ టెక్నాలజీ ఏక్ట్, 2000 (Information Technology Act, 2000), తదితర చట్టపరమైన నియమాలు తప్పనిసరిగా పాటించాలి.

d. బ్యాంకులు, ఖాతాదారుల అకౌంట్ వివరాలు, మరియు ఇతర సమాచారం గోప్యంగా ఉంచాలి. ఇంటర్నెట్ బ్యాంకింగ్ విషయానికి వస్తే, ఎన్నో కారణాలవల్ల, ఇది కష్టంఅవుతుంది. పలు జాగ్రత్తలు తీసుకున్నా, హ్యాకింగ్/ సాంకేతిక లోపాలవల్ల గోప్యతకు భంగం కలగడం, సేవల నిరాకరణ జరిగే ప్రమాదం, ఎక్కువ అవుతుంది. అందువల్ల, బ్యాంకులు ఇటువంటి ప్రమాదాల నివారణకై తగిన చర్యలు తీసుకోవాలి.

III. అంతర్గత నియంత్రణా విధానం (Internal Control System)

ఇంటర్నెట్ బ్యాంకింగ్ సదుపాయం ప్రారంభించే ముందు బ్యాంకులు, పటిష్ఠమైన అంతర్గత పర్యవేక్షణ, ఆడిట్ వంటి వ్యవస్థలు ఏర్పాటు చేయాలి. ఇంతేగాక, డాటా యొక్క యథార్థత/భద్రత, ఖాతాదార్ల గోప్యత, కాపాడడానికి, తగిన విధానాలు రూపొందించాలి. ఖాతాదార్లు ఇంటర్నెట్ ద్వారా చేయగలిగిన లావాదేవీలపై నగదు పరిమితి విధించవచ్చు.

అంతర్గత నియంత్రణా విధానం ఈ క్రింది విషయాలను పరిగణించాలి.

a. **అధికారుల బాధ్యతలు/సంస్థాగత వ్యవస్థ:** అంతర్గత నియంత్రణా వ్యవస్థ సమర్థవంతంగా పనిచేసేలా చూడడం, బోర్డ్ ఆఫ్ డైరెక్టర్ల/ ఉన్నత యాజమాన్యం యొక్క కర్తవ్యం. బోర్డ్ ఆడిట్ కమిటీలో, ఒక నిర్దేశిత సభ్యునికి, ఇన్ఫర్మేషన్ సిస్టంలు, వాటి నియంత్రణ, ఆడిట్ పై స్పష్టమైన అవగాహన ఉండాలి.

b. **ఆడిట్ వ్యవస్థ లో, ఐ ఎస్ ఆడిట్ ఒక భాగమై ఉండాలి:** ఐ ఎస్ ఆడిట్, అంతర్గత ఆడిట్ లో ఒక అభిన్నమైన భాగంగా ఉండాలి. ఆడిట్ చేయడానికి, అవసరమైనప్పుడు న్యాయ సంబంధమైన సాక్ష్యాల్ని సమర్పించడానికి, వివాదాల పరిష్కారానికి, పనికివచ్చే స్పష్టమైన ఆడిట్ ట్రైల్ (audit trail) కోసం, అనువైన వ్యవస్థను ఏర్పాటు చేయాలి.

c. **నివేదికలు, అనుసరణ :** సెక్యూరిటీ సిస్టంలో, వ్యవస్థలో అతిక్రమణలని, వైఫల్యాలని పై అధికారులకు, ఆడిట్ కమిటీకి తెలియపరచే ఒక వ్యవస్థ ఉండాలి. ఐ ఎస్ ఆడిటర్లు,

తాము జరిపిన ఆడిట్ ప్రక్రియపై ఒక నివేదికను తయిరుచేసి, బ్యాంక్‌తో చర్చించి, తగిన వివరణలు కోరతారు. సహకార బ్యాంకులు, ఆడిట్ లో బయటపడిన విషయాలపై, నిర్ణీత కాలంలో అనుసరణ చర్యలు తీసుకోవాలి. తీవ్రమైన వైఫల్యాలని, బోర్డ్ ఆఫ్ డైరెక్టర్లకు తెలియజేయాలి.

సైబర్ భద్రతకు సంబంధిచిన సంఘటనలని, బోర్డ్ కు, ఉన్నత యాజమాన్యానికి, RBI/NABARD లకు, తమకుతామై, నివేదించడానికి, బ్యాంకులు, ఒక విధానాన్ని రూపొందించాలి.

IV. ఇతర అంశాలు, వెల్లడింపులు

ప్రస్తుతం బ్యాంకులపై ఉన్న నియంత్రణా వ్యవస్థ, ఇంటర్నెట్ బ్యాంకింగ్ కు కూడా వర్తిస్తుంది. ఈ సందర్భంగా ఈ క్రింది విధంగా సూచించడమైనది:

a. ఇంటర్నెట్ బ్యాంకింగ్ ద్వారా సౌకర్యాలు, ఖాతాదార్లకు మాత్రమే పరిమితంచేయాలి.
b. దేశీయ కరెన్సీ ఉత్పత్తులకే ఈ సేవలు పరిమితం.
c. ఇంటర్నెట్ బ్యాంకింగ్ లో గల కర్తవ్య/బాధ్యతలను, ప్రమాదాలను ఖాతాదార్లకు తెలియచేయాలి.
d. ఇంటర్నెట్ బ్యాంకింగ్ సౌకర్యాన్ని కలిగించేముందు, బ్యాంకులు KYC నిబంధనలు, AML ప్రమాణాలు PMLA 2002 నియమాలను పాటించాలి.

అనుబంధం -II

ఇంటర్నెట్ బ్యాంకింగ్ - భద్రతా అంశాలు:

1. సహకార బ్యాంకులు, వెబ్ అప్లికేషన్లకు సంబధించి తగిన భద్రతా చర్యలు తీసుకొనవలెను.
2. వెబ్ అప్లికేషన్లలో, ముఖ్యమైన సమాచారాన్ని, HTML హిడెన్ ఫీల్డ్స్, కూకీస్, వంటి, లేక ఇతర ఖాతాదారులకి అందుబాటులో ఉండే స్థానాల్లో, నిలువ చేయరాదు. ముఖ్యమైన వెబ్ అప్లికేషన్ల ద్వారా ఆన్-లైన్ కార్యకలాపాలు సాగించేటప్పుడు, కనీసం SSL v3, లేక ఎక్స్టెండెడ్ వేలిడేషన్ - SSL/TLS 1.0 128 స్థాయి, బిట్ ఎన్క్రిప్షన్ వినియోగించాలి.
3. పనిలో అంత రాయంకలిగితే, తిరిగి ప్రారంభించడానికి, యూజర్ ఐడెన్టిఫికేషన్, ఆథెన్ టికేషన్, ఆథరైజేషన్, ఇంతేగాక పటిష్టమైన సర్వర్ సైడ్ వేలిడేషన్ తిరిగి చేయవలెను.
4. సహకార బ్యాంకులు, వివిధ స్థాయిల్లో, పటిష్ఠమైన గట్టి భద్రతా చర్యల ద్వారా డిఫెన్స్-ఇన్-డెప్త్ (defense-in-depth) వ్యూహాన్ని ఆచరించాలి.

ఇంటర్నెట్ బ్యాంకింగ్ కై ఆంథెన్టికేషన్

1. ఆథెన్టికేషన్ విధానంలో మూడు ముఖ్యాంశాలు (basic factors):
   ఉపయోగించేవారికి తెలిసినవి – (ఉదా: పాస్ వర్డ్, PIN)
   ఉపయోగించేవారు కలిగియున్న వి- (ఉదా: ATM కార్డ్ /స్మార్ట్ కార్డ్)
   ఉపయోగించేవారివి – (ఉదా: బయోమెట్రిక్ వేలిముద్రలు)

2. పలు అంశాల (multifactor), ఆథెన్టికేషన్ విధానాలు సరిగా రూపొందించి, ఆమలుచేస్తే, మోసాలు నివారించడానికి. ఖాతాదార్ల వివరాల/ఖాతాల, లావాదేవీల గోప్యత కాపాడడానికి నమ్మకంగా ఉపయోగపడతాయి. బ్యాంకులు/ వారి ఖాతాదార్లపై, ఫిషింగ్, కీ లాగింగ్, స్పై

వేర్/మాల్‌వేర్ వంటి అంతర్జాల దాడులను తిప్పికొట్టి, ఇంటర్నెట్ బ్యాంకింగ్ పై ఖాతాదార్ల విశ్వాసాన్ని బలపరచడమే, రెండు అంచెల ఆథెన్‌టికేషన్ యొక్క ముఖ్య లక్ష్యం.

ఇంటర్నెట్ బ్యాంకింగ్ - రెండు అంశాల ఆథెన్‌టికేషన్ (two-factor authentication) మరియు ఇతర భద్రతా చర్యల ఆచరణ:

a. పెరుగుతున్న సైబర్ దాడులు, వాటి పరిణామాల దృష్ట్యా, బ్యాంకులు, నగదు బదిలీలకు టూ ఫేక్టర్ ఆథెన్‌టికేషన్ అమలు చెయ్యాలి.

b. కలుగగల నష్టాల్ని, సంస్థ యొక్క ఇంటర్నెట్ బ్యాంకింగ్ సిస్టమ్ ని, ఖాతాదారు శ్రేణిని (వ్యక్తిగత / కార్పొరేట్/ వాణిజ్య), వారి లావాదేవీల తరహాని (బిల్ పేమెంట్/నగదు బదిలీ), వాటి పరిమాణాన్ని, ఖాతాదారు వివరాల ప్రాధాన్యతనీ బట్టి అంచనా వేసి, యోగ్యమనుకొన్న ఆథెంటికేషన్ విధానాన్ని అమలుపర్చాలి.

c. ఆథెన్‌టికేషన్ విధానాలు విజయవంతమవాలంటే, సాంకేతిక అంశాలేగాక, ఇతర విధానాలు, ప్రక్రియలు, నియంత్రణలు సముచితమైనవి అయి ఉండాలి. బ్యాంకులు, ఖాతాదార్ల అగీకారం, సౌలభ్యం, నమ్మిక, వ్యాపారం పెరుగుదల, ఇతర సిస్టమ్స్ తో సంధానించగలిగే వెసులుబాటు తదితర అంశాలు కూడా పరిశీలిస్తే, ఆథెన్‌టికేషన్ విధానం సమర్ధవంతంగా పనిచేస్తుంది.

d. అసిమెట్రిక్ క్రిప్టోసిస్టమ్ (asymmetric crypto system), హ్యాష్ ఫంక్షన్ (hash function) ఉపయోగించకపోతే, చట్ట రీత్యా చిక్కులు రావచ్చు. నగదు బదిలీ వంటి ముఖ్యమైన లావాదేవీలు జరిపేటప్పుడు, కనీసం, టూ ఫేక్టర్ - మొదటిది ఐ డి/ పాస్ వర్డ్, రెండు (a) డిజిటల్ సంతకం (డిజిటల్ సర్టిఫికేట్ మరియు ప్రైవేట్ 'కీ' గలిగిన టోకెన్) లేదా, (b) వన్ టైమ్ పాస్‌వర్డ్ (OTP)/ డైనమిక్ ఏక్సెస్ కోడ్ (SMS, మొబైల్ ఫోన్, హార్డ్‌వేర్ టోకెన్) కలిగిన ఆథెన్‌టికేషన్ అమలుపర్చాలి (ప్రత్యేకించి కార్పొరేట్ ఖాతాదార్లకు).

e. లావాదేవీల పరిమితి మించినపుడు/ క్రొత్త అకౌంట్లు జతచేసినప్పుడు/ 'పేయీ' గా బయటివారి పేరును నమోదు చేసినప్పుడు/ ఖాతా వివరాలు మార్చినప్పుడు/ లేదా నగదు బదిలీ పరిమితి మార్చినప్పుడు, ఆన్‌లైన్ ప్రక్రియలు మరింత సురక్షితంగా సాగించడానికి రెండో మార్గం ద్వారా (టెలిఫోన్, SMS, ఇ-మైల్ మొదలైనవి) రూఢి పరుచుకోవాలి. ఈ చర్యలు నిర్ణయించేముందు, వాటి సమర్థత, ఖాతాదార్ల ఇష్టాయిష్టాలు కూడా ఆలోచించాలి.

f. పరస్పరం అంగీకరించిన ఆథెన్‌టికేషన్ ప్రోటోకాల్స్ ద్వారా, ఖాతాదార్లు కూడా కొన్ని సురక్షా విధానాల ద్వారా (వ్యక్తిగత హామీ సందేశాలు/ చిత్రాలు/ చాలెంజ్ రెస్పాన్స్ కోడ్ మరియు/ లేదా SSL) బ్యాంక్ వెబ్‌సైట్ ను ఆథెంటికేట్ చెయ్యవచ్చు. ఇటీవలి కాలంలో, EV-SSL సర్టిఫికేట్లు విరివిగా ఉపయోగిస్తున్నారు. ఇవి, అధిక రక్షణగల బ్రౌజర్లలో, వెబ్ సైట్ సంస్థలను స్పష్టంగా గుర్తించగలవు. అయితే, SSL, ట్రాన్స్‌పోర్ట్ లేయర్ లోని (transport layer) 'ఇన్-ట్రాన్సిట్' డాటాని (in transit data) మాత్రమే ఎన్‌క్రిప్ట్ చేయగలదు కాని, అప్లికేషన్ లేయర్ (application layer) లోని, ఎండ్-టు-ఎండ్ డాటా ని (end-to-end) ఎన్‌క్రిప్ట్ చేయలేదు, అని గమనించాలి.

g. ఆథెంటికేట్ చేయబడ్డ సెషన్, ఎన్‌క్రిప్షన్ ప్రోటోకాల్ తోసహా, ఖాతాదారు వ్యవహారం జరుపుతున్నంతసేపూ కొనసాగాలి. ఒకవేళ అంతరాయం కలిగితే సేషన్‌ను ముగించి, ఆతరువాత సదరు లావాదేవీలని పరిష్కరించాలి లేదా రివర్స్ చేయాలి. ఖాతాదారుకు ఈ సంగతి సెషన్ ముగింపు సమయం లో లేదా ఆ వెంటనే ఇ-మైల్, టెలిఫోన్ ద్వారా, లేదా వేరే ఏదేని విధంగా తెలియజేయాలి.

h. బ్రాంచ్ నుండి అభ్యర్థన వస్తేనే మొబైల్ నంబరు లో మార్పులని చేయాలి.

i. వర్చువల్ కీబోర్డ్ అమలు చేయ్యాలి.

j. క్రొత్త లబ్ధిదారులను చేర్చుకొన్నప్పుడు, వారి SMS, ఇ-మైల్ అలెర్ట్ల విషయంలో కొంత సమయ విరామం పాటించాలి.

k. ఖాతాదార్లకు, వారి వ్యక్తిగత కంప్యూటర్లను కాపాడుకోవడానికి అవసరమైన భద్రతా చర్యలు ఆచరించమని, సూచించాలి, ఇంటర్నెట్ కఫేల నుండి ఆర్థిక లావాదేవీలు జరపవద్దని సలహా ఇవ్వాలి.

l. దీనితోబాటు, నష్ట ప్రమాదం ఉందనిపించిన లావాదేవీలను పర్యవేక్షించేందుకు ఒక విధానాన్ని అమలు చెయ్యాలి.

m. నిర్ణయించిన కాలం తరువాత, తిరిగి ఆథెన్‌టికేట్ చేస్తేతప్ప, ఆన్‌లైన్ సెషన్, దానంతట అదే ముగిసి పోవాలి. దీనివల్ల, హ్యాకర్లు, సెషన్ అంతులేకుండా పొడిగించే ప్రమాదం వారించబడుతుంది.

n. నిజమైన మల్టి-ఫ్యాక్టర్ ఆథెన్‌టికేషన్ అంటే, మూడింటి నుంచి, రెండు సొల్యూషన్‌లు కలిగి ఉండాలి. ఒకే శ్రేణి నుంచి, వివిధ సందర్భాల్లో, మల్టిపుల్ సొల్యూషన్‌స్ ఉపయోగించడం, వాస్తవానికి, మల్టి-ఫ్యాక్టర్ ఆథెంటికేషన్ అనబడదు.

o. టూ-ఫ్యాక్టర్ ఆథెన్‌టికేషన్ లో అంతర్భాగంగా బ్యాంకులు, మ్యాన్ ఇన్ ది మిడిల్ (MITM), మ్యాన్ ఇన్ ది బ్రౌజర్ (MITB) , మ్యాన్ ఇన్ ది అప్లికేషన్, దాడులను నివారించడానికి తగిన చర్యలు తీసుకోవాలి.

p. MITM దాడులు అరికట్టాడానికి, బ్యాంకులు ఈ క్రింద పేర్కొన్న భద్రత/నియంత్రణ చర్యలు పరిశీలించి, యోగ్యమనిపించినవాటిని, ఆచరణలో పెట్టాలి:

(i) **క్రొత్త పేయీలను చేర్చడానికి నిర్దుష్ఠమైన OTP:** ప్రతి క్రొత్త 'పేయీను', అనుమతించడానికి ఖాతాదారునుండి రెండో మార్గం ద్వారా వచ్చిన **OTP** పై ఆధారపడాలి, దీనిలో, 'పేయీ' వివరాలుఉండాలి. లేదా, బ్యాంక్ లోని లిఖిత పత్రాలనుండి, , ఖాతాదారు వ్రాతపూర్వకంగా చేసిన సంతకాన్ని రూఢి పరచుకోవాలి.

(ii)**చెల్లింపులు, నగదు బదిలీలకు, వ్యక్తిగత OTP లు:**

ప్రతి నగదు లావాదేవీకి, లేక అనుమతించిన జాబితాలో, ఖాతాదారు నిర్ణయించిన నగదు పరిమితి మీరిన, లావాదేవీలకు, ఒక క్రొత్త **OTP** తప్పనిసరి చెయ్యాలి.

(iii) **OTP సమయం:** చాలెంజ్-బేస్‌డె (challenge- based) మరియు టైం-బేస్‌డ్ (time-based) **OTP** ల సమయం, ఉపయోగించేవారి ప్రమేయం లేకుండా, బ్యాంక్ నియంత్రిస్తుంది గనుక, పటిష్ఠమైన భద్రత నిస్తాయి. బ్యాంకులు ఈ సమయాన్ని, సర్వర్ టైమ్ కి ముందు/తరవాత 100 సెకండ్లకు మించి అనుమతించరాదు. ఈ సమయంఎంత తక్కువ ఉంటే, OTP దుర్వినియోగం అంతమేరకు తగ్గుతుంది.

(iv) **చెల్లింపులు, నగదు బదిలీలకు భద్రత:**

చెల్లింపులు నగదు బదిలీలలో, మిడిల్ మ్యాన్ దాడులు చేసి, అనధికార మార్పులు చేయడం, లావాదేవీలను చొప్పించడం వంటి చర్యలు కనుగొనేందుకు డిజిటల్ సంతకాలు, కీ బేస్‌డ్ మెసేజ్ ఆథెన్‌టికేషన్ కోడ్‌లు (KMAC) ఉపయోగించవచ్చు. అయితే, హార్డ్‌వేర్ టోకెన్ ఉపయోగించే ఖాతాదారు, వన్ టైమ్ పాస్‌వర్డ్ కీ, డిజిటల్ సంతకానికీ మధ్య ఉన్న భేదాన్ని గుర్తించగలగాలి. డిజిటల్ సంతకం దేనికిచేశారో అర్థంచేసుకోవాలి. అంటే, టోకెన్, స్పష్టంగా 'పేయీ' అకౌంట్ నంబరు, చెల్లింపు మొత్తాన్ని సూచించాలి. దీని నుంచి, డిజిటల్ సంతకం చేయడానికి హ్యాష్ వేల్యూ పొందవచ్చు. **OTP** సృష్టించడానికి, లావాదేవీల సంతకానికి, వేరు వేరు క్రిప్టో కీలను (crypto keys) వినియోగించాలి.

(v) ఇంటర్నెట్ బ్యాంకింగ్ లో చెల్లింపు నిలుపుదలకు అవకాశం తక్కువ. అందుకని, చెల్లింపు నిలుపుదల ఆదేశాలు ఏ సందర్భాల్లో, ఎంత సమయం లోపు అంగీకరించబడతాయో, ఖాతాదారులకి వివరంగా తెలియచేయాలి.

(vi) వినియోగదారుల రక్షణ చట్టం, 1986 (Consumer Protection Act, 1986) బ్యాంకింగ్ సేవలకు కూడా వర్తిస్తుంది. అందువల్ల, ఇంటర్‌నెట్ బ్యాంకింగ్ వినియోగించుకొనే ఖాతాదార్లకు, వారి హక్కులు/ బాధ్యతల గురించి వివరంగా

తెలియచెయ్యాలి. సాంప్రదాయిక బ్యాకింగ్ లో వలె కాకుండా, ఇంటర్నెట్ బ్యాంకింగ్ లో హ్యాకింగ్ వల్ల జరగబోయే అనుమతి లేని చెల్లింపుల వల్ల, సాంకేతిక లోపాలకారణంగా, సేవల వైఫల్యం మొదలైనవాటివల్ల కలుగబోయే నష్టాలను, అంచనావేసి, వాటినుండి బ్యాంకులు తమనుతాము రక్షించుకోవాలి.

(vii) బ్యాంక్ వెబ్సైట్ల లోని హైపర్లింక్స్, బ్యాంక్ ప్రతిష్ఠకు భంగంరానీయకూడదు. వీటివల్ల, ఖాతాదార్లు, ఏదేని బ్యాంకింగ్ కు సంబంధం లేని ఉత్పత్తులను, బ్యాంక్ ప్రోత్సహిస్తోందని భావించరాదు.

ఏదైన చెల్లింపు ఒప్పందం ఉన్న పోర్టల్స్ యొక్క హైపర్ లింకులు మాత్రమే, బ్యాంక్ వెబ్సైట్ లో ఉండాలి. ఇతర పోర్టల్స్ యొక్క హైపర్లింక్స్, సాధారణంగా, తమనుంచి ఖాతాదార్ల కొనుగోళ్ళకు సంబంధించిన సమాచారాన్ని తెలపడానికిమాత్రమే ఉద్దేశించబడాతాయి. బ్యాంకులు, ఖాతాదార్ల కొనుగోళ్ళకు సంబంధించి, ఇతర వెబ్సైట్ల అభ్యర్థనల విషయంలో, సిఫారసు చేయబడ్డ భద్రతా సూచనలని పాటించాలి.

(viii) **రెండవ మార్గంలో ప్రకటన / ధృవీకరణ**

ఖాతాదారు నిర్ణయించిన నగదు పరిమితిమీరి జరిపిన ప్రతి చెల్లింపు, నగదు బదిలీ వివరాలు, రెండో మార్గం ద్వారా ఖాతాదారుకు తెలియపరచాలి

(ix) **SSL సర్వర్ సర్టిఫికేట్ హెచ్చరిక:** ఇంటర్నెట్ బ్యాంకింగ్ ఖాతాదార్లకు, SSL/EV-SSL సర్టిఫికేట్ హెచ్చరికల గురించి, వాటికి ఎలా స్పందించాలి అనే విషయమై అవగాహన కల్పించాలి.

(x) ఖాతాదార్ల లావాదేవీల తీరు గమనించి, దానికి భిన్నంగా ఉన్న లావాదేవీలను నిలుపు చేయాలి/లేదా, ఖాతాదారుయొక్క ధృవీకరణ పొందాలి. ఇందుకై, తగిన పర్యవేక్షణ, నిఘా వ్యవస్థను, సాఫ్ట్వేర్ లో పొందుపరచాలి.