(ریزو بینک آف انڈیا)

www.rbi.org.in

آر بی آئی/2015-16/229

ڈی سی بی آر۔ بی پی ڈی (پی سی بی/ آر سی بی) سرکلر نمبر 6/19.51.026/2015-16

چیف ایگزیکیوٹیو افسر

سبھی پرائمری (دیہی) کوآپریٹیو بینک/ ریاستی اور مرکزی کوآپریٹیو بینک

میڈم/ ڈیر سر

کوآپریٹیو بینکوں کے صارفین کے لئے انٹرنٹ بینکنگ سہولیات

برائے مہربانی ہمارے سرکلر یو بی ڈی بی پی ڈی (ایس سی بی) سرکلر نمبر 1/09.18.300/2011-12 مورخہ ۱۱ ستمبر ۲۰۱۱ جو انٹرنٹ بینکنگ یو سی بی صارفین کے لئے ہے، کا حوالہ دیکھیں جس میں شیڈولڈ دیہی کوآپریٹیو بینک (یو سی بی) نے معیارات پر اظہار اطمینان کرتے ہوئے اپنے صارفین کو روپیوں کے لین دین کی سہولت کے ساتھ انٹرنٹ بینکنگ کی سہولت کی اجازت آر بی آئی سے پیشگی اجازت اور سرکلر یو بی ڈی، بی ڈی (پی سی بی) سرکلر نمبر 21/09.18.300/2014-15 مورخہ ۱۳ اکتوبر ۲۰۱۴ء کو انٹرنیٹ بینکنگ (صرف تصدیق کے لئے) یو سی بی صارفین کی سہولت کے لئے، کی اجازت سبھی یو سی بی کو آر بی آئی کی اجازت کے بغیر (صرف تصدیق کے لئے) کے تحت چند شرائط میں توسیع کرتے ہوئے انٹرنٹ بینکنگ کی سہولت دی تھی۔

(۲) ریاستی کوآپریٹیو بینک (ایس ٹی سی بی) اور ضلع سینٹرل کوآپریٹیو بینک (ڈی سی سی بی) نے اپنے صارفین کو انٹرنٹ بینکنگ کی اجازت نہیں دی تھی جب کہ کچھ ایس ٹی سی بی/ ڈی سی سی بی نے انٹرنٹ بینکنگ سہولت کی اجازت دینے کے لئے گذارش کی تھی جس کے پیش نظر ایس ٹی سی بی/ ڈی سی سی بی کو اپنے صارفین کے لئے انٹرنٹ سہولت فراہم کرانے اجازت دینے کا فیصلہ کیا گیا، یو سی بی کو جاری رہنما ہدایات کا از سر نو جائزہ لینے اور اس معاملہ میں یو سی بی کو جاری قبل کی رہنما ہدایات کو منسوخ کرتے ہوئے نئی رہنما ہدایات کا اجراء کیا جارہا ہے، مندرجہ ذیل کے تحت ترمیم شدہ رہنما ہدایات کا نفاذ بھی کوآپریٹیو بینکوں پر ہوگا۔

(i) انٹرنٹ بینکنگ (صرف تصدیق کے لئے) سہولت

(۳) سبھی لائسنس یافتہ ایس ٹی سی بی، ڈی سی سی بی اور یو سی بی جنہوں نے کور بینکنگ سالوشن (سی بی ایس) نافذ کیا ہے اور انٹرنٹ پروٹوکول ورزن ۶ (آئی پی وی ۶) میں منتقل کیا ہے اور سرکلر کے انیگزر۔ ا کے تحت رہنما ہدایات پر عمل آوری کرتے ہیں انہیں انٹرنٹ بینکنگ (صرف نظریہ) کی اپنے صارفین کے لئے سہولت کی اجازت آر بی آئی سے پیشگی اجازت کے بغیر دی جاتی ہے۔ اتفاق سے صرف نظریہ کے تحت حاصل کردہ سہولیات میں دو فیکٹر مجاز کی ضرورت ہوتی ہے یا ایک وقت پاس ورڈ (او ٹی پی) ہے تو بینک اس سرکلر کے انیگزر ۱۱ میں پیش کردہ حفاظتی بندوبست کو اختیار کر سکتے ہیں جو کہ اس طرح کی خدمات کے لئے مناسب ہے۔

(۴) کوآپریٹیو بینک جو اپنے صارفین کو انٹرنٹ بینکنگ (صرف تصدیق کے لئے) سہولت فراہم کراتے ہیں انہیں اس بات کو یقینی بنانا ہوگا کہ یہ سہولت شخص سے صرف غیر ٹرانزکشنل خدمات مثلاً بیلنس انکواری، بیلنس دیکھنا، اکاونٹ اسٹیمیٹ کی ڈاون لوڈنگ، چیک بک وغیرہ کو جاری کرنے کی گذارش سے متعلق ہے اور آن لائن فنڈ پر منحصر ٹرانزکشن کی اجازت نہیں ہے۔

(۵) انٹرنٹ بینکنگ (صرف تصدیق کے لئے) سہولت شروع کرنے کے ایک ماہ میں کوآپریٹیو بینکوں کو آر بی آئی کے متعلقہ ریجنل آفس (اور ایس ٹی سی بی/ ڈی سی سی بی کے معاملہ میں نبارڈ کو بھی) کو مطلع کرنا ہوگا۔

(ii) ٹرانزکشنل سہولت کے ساتھ انٹرنٹ بینکنگ

(۶) سبھی لائسنسی ایس ٹی سی بی، ڈی سی سی بی اور یو سی بی جنہوں نے سی بی ایس نافذ کر رکھا ہے اور انٹرنٹ پروٹوکول ورزن ۶ (آئی پی وی ۶) میں بھی شامل ہوئے ہیں اور مندرجہ ذیل معیار کو پورا کرتے ہوں تو آر بی آئی سے انٹرنٹ بینکنگ ٹرانزکشنل سہولت سمیت اپنے ایسے صارفین کو فراہم کرانے کے لئے پیشگی اجازت حاصل کرنا ہوگی۔

(الف) سی آر اے آر کو ۱۰ فیصد سے کم نہیں ہونا چاہئے۔

(ب) پچھلے ۳۱ مارچ تک کے مالیاتی پیش رفت سال میں مجموعی رقم روپئے ۵۰ کروڑ یا اس سے زائد ہونا چاہئے۔

(ت) مجموعی این پی اے ۷ فیصد سے کم اور اصل این پی اے ۳ فیصد سے زائد نہیں۔

(ج) رواں مالی سال میں بینک کی اصل آمدنی منافع میں ہو اور پچھلے چار سالوں میں سے کم از کم تین سالوں میں اصل منافع ہونا چاہئے۔

(چ) رواں مالیاتی سال میں سی آر آر/ ایس ایس آر کے رکھ رکھاؤ میں خامی نہیں ہونا چاہئے۔

(ح) بورڈ کے کم از کم دو ماہر ڈائریکٹروں کے ذریعہ داخلی امور پر کنٹرول نظام ہونا چاہئے۔

(خ) گذشتہ دو مالیاتی برسوں میں، جس سال درخواست پیش کی جارہی ہو بینک کی ضوابط کی پابندی اور اس کے اوپر آر بی آئی حکم نامے/ رہنما ہدایات کی خلاف ورزی پر جرمانہ عائد نہیں ہوا ہو۔

(۷) ایس ٹی سی بی، ڈی سی سی بی اور یو سی بی کو مذکورہ بالا معیار کو انٹرنٹ بینکنگ کی توسیع مع ٹرانزکشنل سہولت کی اجازت کے لئے مکمل کرنا ہوگا جس کا ذکر سرکلر کی رہنما ہدایات انیکزر ۱، اور ۱۱، میں درج ہے۔ اس مقصد کے لئے ایس ٹی سی بی، ڈی سی سی بی اور یو سی بی آر بی ریجنل دفتر میں درخواست (اس ٹی سی بی/ ڈی سی سی بی کے معاملہ این اے بی اے آر ڈی (نبارڈ) کے ذریعہ مندرجہ ذیل دستاویزات کے ساتھ پیش کرنا ہوگی۔

(i) انٹرنٹ بینکنگ پالیسی پر بورڈ کی مصدقہ کاپی کے ساتھ آزادانہ آڈیٹر (سی آئی ایس اے ڈگری یافتہ) کی تصدیق جو کہ آئی ٹی اور آئی ایس پالیسی جس کا ذکر آر بی آئی کی رہنما ہدایات میں ہوا ہے کو پورا کرتی ہو۔

(ii) آر بی آئی کو اقرار نامہ پیش کرنا ہوگا اس کے ذریعہ فراہم کردہ خدمات/ پروڈکٹ میں کسی قسم کی تبدیلی نہیں کی جائے گی۔

(iii) کاروباری منصوبہ، لاگت اور منافع تخمینہ، آپریشنل بندوبست مثلاً اختیار کردہ ٹکنالوجی، کاروباری ساتھی، خدمات فراہم کرانے والی تیسری پارٹی اور سسٹم اور کنٹرول طریقہ کار جس کو بینک مینجنگ خطرات سے نمٹنے کے لئے اختیار کر رہا ہے۔

(۸) بینک کو آر بی آئی کے متعلقہ ریجنل آفس (اس ٹی سی بی/ ڈی سی سی بی کے معاملہ میں بھی) ہر ایک خامی یا سیکورٹی سسٹم کی ناکامی اور پیش رفت کی اطلاع دینا ہوگی، جیسا کہ ریزو بینک کو اختیار ہوگا کہ وہ اس طرح کے بینک کے خصوصی آڈٹ/ جانچ کے لئے کمیشن کی تشکیل کا فیصلہ کرے۔

(۹) ایس ٹی سی بی/ ڈی سی سی بی جو کہ پہلے ہی سے انٹرنٹ بینکنگ (صرف تصدیق کے لئے) سہولت اپنے صارفین کو فراہم کرا رہے ہیں انہیں ان رہنما ہدایات کی روشنی میں اپنے سسٹم کا جائزہ لینا ہوگا اور متعلقہ آر بی آئی کے ریجنل آفس کو (این اے بی اے آر ڈی کے ذریعہ) سرکلر کے اجراء کے ایک ماہ کے اندر رپورٹ کرنا ہوگا کہ اس کو کس طرح کی خدمات کی پیشکش کی گئی ہے اور اس نے کس حد تک رہنما ہدایات پر عمل کیا ہے۔

(۱۰) ایس ٹی سی بی/ ڈی سی سی بی جو کہ انٹرنٹ بینکنگ ٹرانزکشنل خدمات پہلے سے ہی فراہم کرا رہے ہیں انہیں صلاح دی جارہی ہے کہ سرکلر میں شامل ہدایات پر عمل کریں اور اپنے بزنس ماڈلس، لاگت/ منافع کا تخمینہ وغیرہ کی تفصیل پیش کریں اور سرکلر کے اجراء کے ایک ماہ کے اندر آر بی آئی کے مصدقہ ریجنل آفس سے منظوری حاصل کریں، اس طرح کی درخواستوں کو نابارڈ کے ذریعہ آر بی آئی کے ریجنل آفس کو ارسال کریں۔

(سوما ورما)

مخلص

پرنسل چیف جنرل منیجر

مسلکات: مذکورہ بالا کے مطابق

کوآپریٹیو بینکوں کے صارفین کے لئے انٹرنٹ بینکنگ سہولت سے متعلق رہنما ہدایات

لائسنس یافتہ ایس ٹی سی بی، ڈی سی سی بی اور یو سی بی اور اپنے صارفین کو انٹرنٹ بینکنگ سہولت فراہم کرانے کے خواہاں ہیں تو انہیں مندرجہ ذیل پر عمل آوری کرنا ہوگی۔

(i) بینک کو بورڈ کی اجازت سے انٹرنٹ بینکنگ کے لئے پالیسی بنانا ہوگی۔

(ii) پالیسی کو بینک کی مجموعی انفارمیشن ٹکنالوجی اور انفارمیشن سیکورٹی پالیسی پر فٹ آنا چاہئے اور ریکارڈ اور سیکورٹی نظام کو یقینی بنانا ہوگا۔

(iii) پالیسی میں وضاحت کے ساتھ ''جانئے اپنے صارف کو'' کی ضروریات کے طریقہ کار کی وضاحت کی جائے۔

(iv) پالیسی میں ٹکنالوجی اور سیکورٹی معیارات کے احاطہ کے ساتھ قانونی ریگولیٹری اور نگرانی کے معاملات کا ذکر انگیزر کے مطابق ایک کیا جائے۔

(v) بینکوں کو مضبوط داخلی کنٹرول بندوبست رکھنا ہوگا اور آپریشنل خطرات پر نظر رکھنا ہوگی جو کہ خدمات کی فراہمی کے دوران درپیش ہو سکتے ہیں۔

(vi) خطرات، ذمہ داریوں اور قابل برداشت عمل جن کا تعلق صارفین سے ہوگا، سہولت کے فراہمی سے قبل قابل قبول شرائط وضع کرنا ہوگی۔

مندرجہ ذیل رہنما ہدایات کا اجراء بینک کے ذریعہ نفاذ کے لئے کیا جارہا ہے۔

(ا) **ٹکنالوجی اور سیکورٹی معیار:**

(الف) کوآپریٹیو بینکوں کو بورڈ آف ڈائریکٹرس کی منظوری سے مناسب انفارمیشن سیکورٹی پالیسی تیار کرنا ہوگی۔ کام کے معاملہ میں انفارمیشن ٹکنالوجی (آئی ٹی) ڈویژن اور انفارمیشن سیکورٹی آئی ایس ڈویژن کی ذمہ داریاں بالکل علاحدہ ہوں گی، انفارمیشن ٹکنالوجی ڈویژن دراصل کمپیوٹر سسٹم کا نفاذ کرے گا جب کہ ایک الگ انفارمیشن سیکورٹی افسر ہوگا جو کہ انفارمیشن سسٹم سیکورٹی کی نگرانی کرے گا، ایک انفارمیشن سسٹم آڈیٹر انفارمیشن سسٹم کا آڈٹ کرے گا۔

(ب) بینکوں کو اپنے بورڈ کی منظوری سے نٹ ورک اور ڈاٹا بیس ایڈمنسٹریٹر کی تقرری آئی ایس آڈٹ پالیسی کی مکمل وضاحت کے ساتھ کرنا ہوگی۔

(ت) ڈاٹا کے لئے لاجیکل ایس کنٹرول، سسٹم اپلیکیشن سافٹ ویر، یوٹی لائیٹر، ٹیلی کمیونیکیشن لائن، لائبریز، سسٹم سافٹ ویئر وغیرہ ایک ترتیب میں ہونا چاہئے۔

(ث) بینکوں کو یہ یقینی بنانا ہوگا کہ انٹرنٹ اور بینک سسٹم میں کوئی براہ راست کنکشن نہیں ہے۔

(ج) بینکوں کے پاس موثر حفاظتی تدابیر سسٹم/نٹ ورک میں پیدا خامی کو دور کرنے کے لئے ہونا چاہئے۔

(چ) اپلکیشن سرور سے متعلق سبھی غیر ضروری خدمات مثلاً فائل ٹرانسفر پروٹوکول (ایف ٹی پی) ٹیلینٹ وغیرہ نقائص ہوں گے، اپلیکیشن سرور کو ای میل سرور سے علاحدہ کرنا ہوگا۔

(ح) سبھی کمپیوٹرس کی پہونچ میں حاصل کردہ میسیج کو بھی بطور سرکاری ریکارڈ رکھنا ہوگا سیکورٹی خلاف ورزی (شبہ یا حملہ) کا بھی ریکارڈ رکھنا ہوگا اور اس کے خلاف کارروائی کرنا ہوگی۔ بینکوں کو دخل اندازی اور حملہ کے خلاف کی گئی کارروائی پر نظر رکھنے کے لئے اور نٹ ورک کے نظام کے لئے ٹولس رکھنا ہوں گے۔ ان ٹولس کا استعمال مسلسل سکورٹی میں ہونے والی خامیوں کو دور کرنے کے لئے کرنا ہوگا، بینکوں کو اپنے سیکورٹی انفراسٹرکچر اور سیکورٹی پالیسیوں کا باقاعدگی سے جائزہ لینا ہوگا اور اپنے تجربہ کی روشنی میں ٹکنالوجی میں تبدیلی کرکے سیکورٹی کی نظام کو مزید بہتر کرنا ہوگا۔

(خ) انفارمیشن سیکورٹی افسر اور انفارمیشن سسٹم آڈیٹر کو سسٹم کا وقفہ وقفہ سے سنجیدہ ٹسٹ لینا ہوگا جس میں شامل ہوگا۔

(ا) پاسورڈ کے استعمال کے لئے پاسورڈ توڑنے والے ٹولس کی جانچ۔

(۲) پروگرام میں بیک ڈور ٹریس کی تلاش۔

(۳) اور کوڈ سسٹم جس کے استعمال سے ڈی ڈی ایس اور ڈی ایس پر حملہ ہوتا ہے، کی جانچ کرنا۔

(۴) سافٹ ویر میں ہونے والی عام خرابیوں خاص طور سے بروسر اور ای میل سافٹ ویئر اکزاسٹ کی جانچ۔

(۵) باہری ماہرین (جنہیں اکثر صورتی ہیکرس کہا جاتا ہے) کی مدد سے سخت امتحان کا بندوبست۔

(د) فزیکل معلومات کنٹرول پر سختی سے عمل درآمد، فزیکل سیکورٹی کو بھی انفارمیشن سسٹم اور سائٹس اگر چہ وہ گھروں تک محدود ہوں داخلی اور خارجی دونوں حملوں کے خلاف احاطہ کرنا ہوگا۔

(ذ) بینکوں کو باقاعدگی سے اپنا انفرااسٹرکچر اور بینکنگ بیک اپ ڈاٹا رکھنا ہوگا، بیک اپ ڈاٹا کو مقررہ وقفہ میں جانچ کرنا چاہئے تاکہ ٹرانزکشن کی ریکوری کو بغیر نقصان ایک مہینہ وقت میں بینک کی سیکورٹی پالیسی کے تحت یقینی بنایا جاسکے۔ کاروباری سرگرمی کو ڈزاسٹر ریکوری سائٹوں پر یقینی بنانا ہوگا ان سہولیات کی جانچ بھی وقفہ سے کرنا ہوگی۔

(ر) قانونی مقصد سے سبھی درخواستوں کا باقاعدگی سے ریکارڈ رکھنا ہوگا یہ بھی لازمی ہوگا سبھی پائے جانے اور پہنچ جانے والے میسجوں کو کوڈ میں تبدیل اور غیر تبدیل شکل میں محفوظ رکھا جائے۔

(س) سسٹم کے استعمال اور عمومی آپریشن سے قبل سیکورٹی انفرااسٹرکچر کی باقاعدگی سے جانچ کرنا ہوگی، بینکوں کو نئے ورزن کے ذریعہ سسٹم کو بہتر بنانا ہوگا تاکہ بہتر سیکورٹی اور کنٹرول میں آسانی ہو۔

(ش) کمپیوٹر اور ٹیلی کمیونیکیشن خطرات اور کنٹرول سے تعلق آر بی آئی کی رہنما ہدایات جس کا اجراء سرکلر ڈی بی ایس سی او آئی ٹی سی بی سی 10/31.09001/97-98 مورخہ ۶ر فروری 46/17:36:00/97-98 یو بی ڈی نمبر 1998 مورخہ مارچ ۱۹۹۸ء۳۰ اور سرکلر ڈی بی ایس بی اور ڈی ٹی سی بی سی نمبر 6/31.02.008/2010-11 مورخہ ۲۹ر اپریل ۲۰۱۱ء کے تحت ہوا جس میں انفارمیشن سیکورٹی الکٹرانک بینکنگ ٹکنالوجی ایک مینجمنٹ اور سائبر جلسازی چیئرمین: مسٹر جی گوپالاکرشن، ایگزیوٹیو ڈائریکٹر سے ورکنگ گروپ کی سفارشات سے متعلق ہے۔ بینکوں کو صلاح دی جاتی ہے کہ ان سفارشات پر عمل کریں اور انٹرنٹ بینکنگ میں بھی اسے نافذ کریں۔

(ص) ایس ٹی سی بی/ ڈی سی سی بی کے معاملہ میں آئی اس آڈٹ پالیسی سے متعلق رہنما ہدایات نابارڈ کے سرکلر نمبر بی ڈی ایس ایچ او پی او ایل نمبر 2-3634/01 مورخہ 15-2014 فروری کا ہے 2015 پر بھی عمل آوری ہوگی۔

(۱۱) **قانونی معاملات**

(الف) بینک انٹرنٹ بینکنگ سہولت اپنے صارف کو بطور متبادل خصوصی تحریر یا مجاز الکٹرانک درخواست مع حصولیابی رسید پر فراہم کرا سکتے ہیں۔

(ب) قانونی صورتحال کے مطابق صارف کے ذریعہ انٹرنٹ بینکنگ حاصل کرنے سے قبل بینکوں کو صارف کی شناخت اور اس کی حیثیت کی جانچ کرنا ہوگی اس کے بعد اگر انٹرنٹ پر اکاونٹ کھولنے کی گذارش قبول کی جاتی ہے تو اکاونٹ کی شناخت کی جانچ اور کے وائی سی رہنما ہدایت پر عمل آوری کے بعد ہی کھولا جائے گا۔

(ج) قانونی لحاظ سے سیکورٹی ضابطہ کے تحت استعمال کرنے والے کی ضرورت کے پیش نظر دستخط کے متبادل کے طور پر قانونی شناخت کے بعد اختیار دیا جاسکتا ہے، انفارمیشن ٹکنالوجی ایکٹ ۲۰۰۰ کے تحاویز اور دیگر قانونی ضروریات کے پیش نظر انٹرنٹ بینکنگ فراہم کراتے وقت بہت احتیاط اور باریک بینی کی ضرورت ہوتی ہے۔

(د) موجودہ وقت میں بینکوں پر یہ لازم ہے کہ صارف کے کھاتے/ اطلاعات سے متعلق رازداری برقرار رکھیں، انٹرنٹ بینکنگ کے تحت بینک

مختلف فیکٹری کے اکاونٹ کے سلسلہ میں اس طرح کے خطرات کا سامنا نہیں کریں گے۔

سبھی مناسب احتیاط کے علاوہ بینک اکاونٹ کی رازداری پر لاحق خطرات کے لئے صارفین کی ذمہ داری کو ظاہر کر سکتے ہیں، خدمات کی فراہمی سے انکار کر سکتے ہیں، اس کا سبب بینکنگ/تکنالوجیکل غیر فعالیت ہوسکتا ہے، بینکوں کو اس طرح کے خطرات سے نپٹنے کے لئے حکمت عملی اختیار کرنا پڑے گی۔

(III) داخلی کنٹرول سسٹم

انٹرنٹ بینکنگ کی پیشکش سے قبل بینکوں کو مضبوط داخلی کنٹرول سسٹم کو فروغ دینا ہوگا، اس کے لئے داخلی معائنہ/ انٹرنٹ بینکنگ سے متعلق آڈٹ سسٹم کو یقینی بنانا ہوگا کہ ڈاٹا، صارف کی رازداری اور ڈاٹا کی حفاظت کی جائے گی بینکوں کو صارفین کے لئے انٹرنٹ بینکنگ کے لئے ٹرانزکشن کی حد مقرر کرنا ہوگا۔

داخلی کنٹرول سسٹم میں مندرجہ ذیل شامل ہیں۔

(الف) کردار اور ذمہ داری/ ادارہ جاتی ڈھانچہ: بورڈ آف ڈائریکٹرس اور سینئر انتظامیہ اس کے لئے ذمہ دار ہوگی کہ داخلی کنٹرول کو موثر طور پر چلایا جائے بورڈ کی آڈٹ کمیٹی کو انفارمیشن سسٹم، کنٹرول اور آڈٹ معاملات جاننے والے ایک ممبر کو ذمہ داری سونپے۔

(ب) آڈٹ پالیسی بشمول آئی ایس آڈٹ: آئی ایس آڈٹ بینکوں کے داخلی آڈٹ کا ایک بنیادی حصہ ہوگا۔ بینک سسٹم کا نفاذ اس بات کو یقینی بنانے کے لئے کریں کہ ایک آڈٹ مشق کے ذریعہ بہترین آڈٹ کے طریقہ کار کو رائج کیا جا سکے، جب ضرورت ہو تو فورنسک گواہی پیش کی جا سکے اور متنازعہ کا حل نکالنے میں مدد مل سکے۔

(ج) رپورٹنگ اور عمل آوری: اعلیٰ اتھارٹی کی سرگرمیوں کی رپورٹنگ کے لئے ایک طریقہ کار کی شمولیت، سیکورٹی سسٹم اور پیش رفت میں کسی قسم کا نقص یا ناکامی پر اگلی اعلیٰ اتھارٹی اور آڈٹ کمیٹی کو رپورٹ کی جائے گی۔

آئی ایس آڈیٹرس آڈٹ کا خلاصہ آڈٹ فائنڈنگ، آڈٹ کرنے والوں سے تبادلہ خیال کے بعد تیار کریں گے، کو آپریٹیو بینک آڈٹ فائنڈنگ پر عمل آوری کے لئے وقت مشورہ کی پالیسی مقرر کریں گے۔

بورڈ کے ڈائریکٹروں کے لئے لازمی ہے کہ وہ سیکورٹی اور پیش رفت کے دوران راہ پانے والی بڑی غلطیوں کو معلوم کریں۔

بینک اہم سائبر سیکورٹی واقعات کو بورڈ/ سینئر منیجمنٹ/ آر بی آئی/ نابارڈ کو سرعت سے پہونچانے/ رپورٹنگ کے لئے رابطہ منصوبہ تیار کریں۔

(iv) دیگر معاملات اور اطلاعات کو عام کرنا:

بینکوں کے ریگولیٹری فریم ورک کی توسیع انٹرنٹ بینکنگ پر بھی ہوگی، اس سلسلہ میں یہ صلاح دی جاتی ہے۔

(الف) انٹرنٹ بینکنگ کے تحت پروڈکٹ صرف کھاتہ داران کیلئے ممنوع رہیں گے۔

(ب) سروس میں صرف مقامی کرنسی پروڈکٹ شامل ہوں گے۔

(ج) کو آپریٹیو بینکوں کو انٹرنٹ کے ذریعہ بینکنگ کے دوران صارفین کو خطرات، ذمہ داریوں، جوابدہی کو عام کرنا ہوگا۔

(د) انٹر بینکنگ کی پیشکش کے وقت پی ایم ایل اے ۲۰۰۲ کے تحت جاری ہدایات جن کا تعلق کے وائی سی رہنما ہدایات/ اے ایم ایل معیارات سے ہے بینکوں کے لئے جاننا ضروری ہوگا۔

انٹرنیٹ بینکنگ، سیکورٹی کا خاکہ:

(ا) کو آپریٹیو بینکوں کو ضرورت ہے کہ اپنے ویب ایپلکیشن کے حفاظتی بندوبست کو نافذ کرنے کو یقینی بنالیں اور مختلف ویب سیکورٹی کو مضبوط بنانے کے لئے مناسب اقدامات کریں۔

(۲) ویب ایپلکیشن کے ایچ ٹی ایم ایل کی خفیہ فیلڈس کو کیز یا کوئی دیگر سائلنٹ سائٹ اسٹوریج میں حساس انفارمیشن اور ڈاٹا کو محفوظ ہیں کیا جانا چاہئے۔ حساس ویب ایپلیکیشن کو ایس ایس ایل وی ۳ یا ایکسٹنڈڈ ویلیڈیشن، ایس ایس ایل/ ٹی ایل ایس 1.0.12008 میں کوڈ کی شکل بھی آن لائن سرگرمیوں کو منتقل کر دینا چاہئے۔

(۳) تسلسل ختم کرنے کے بعد کسی بھی مشن کے از سر نو قیام کے وقت یوزر شناخت مجازیت، استحقاق کی ضرورت ہوتی ہے ایسا کرنے سے سرور کے کام میں اضافہ ہوگا۔

(۴) کارپوریٹ بینکوں کے لئے لازمی ہے کہ ٹکنالوجی کی مختلف سطحوں پر چاق و چوبند حفاظتی تدبیر کو اپنانے کے لئے گہری دفاعی حکمت عملی اختیار کریں۔

انٹرنٹ بینکنگ کیلئے مجاز عمل

(۱) مجاز عمل کا تعلق تین بنیادی فیکٹروں سے ہوتا ہے:

وہ چیزیں جنہیں استعمال کرنے والا جانتا ہے (مثلاً پاسورڈ، پی آئی این)

وہ چیزیں جنہیں استعمال کرنے والا رکھتا ہے (مثلاً اے ٹی ایم کارڈ، اسمارٹ کارڈ) اور

کچھ چیزیں استعمال کرنے والے کے لئے (مثلاً بائیومیٹرک کیریکٹر اسٹک، مثلاً انگلیوں کے نشان)

(۲) قاعدہ سے ڈیزائن اور نافذ کیا گیا مجاز عمل جعلسازی کو پکڑنے میں زیادہ بھروسہ مند اور سمجھوتہ میں زیادہ وقت طلب ہوتا ہے، دو فیکٹر والے مجاز عمل کا اہم اصول صارف کے اکاونٹ ڈاٹا اور ٹرانزکشن تفصیل کی حفاظت کرنا اور مختلف سائبر حملوں مثلاً پشنگ، کے لاگنگ، اسپائی ویئر/ مال ویکر اور دیگر انٹرنٹ منحصر جعلسازی کے طرف سے بینک اور ان کے صارفین کو محفوظ رکھنا ہے۔

دو فیکٹر مجازیت اور دیگر سیکورٹی پیمانوں کا انٹرنٹ بینکنگ میں نفاذ:

(الف) سائبر حملوں کے تناظر اور ان کے اثرات کے تناظر میں بینک انٹرنٹ بینکنگ کے ذریعہ رقم کی منتقلی میں دو فیکٹر مجازیت کے نافذ کر سکتے ہیں۔

(ب) مناسب مجاز طریقہ کار نفاذ انٹرنٹ بینکنگ سسٹم کے ادارہ کے جانب سے خطرات کے اندیشہ کی بنیاد پر ہوگا۔ یہ خطرات صارف کی اقسام (مثلاً فردہ یا کارپوریٹ/ کمرشیل صارف کی ٹرانزکشنل صلاحیت (مثلاً بل کی ادائیگی، فنڈ کی منتقلی) کی بنیاد پر ہو سکتے ہیں، اس کی وجہ صارف کی انفارمیشن کی حساسیت اور ٹرانزکشن کا حجم بھی ہو سکتا ہے۔

(ج) ٹکنالوجی فیکٹر سے پرے مخصوص مجاز طریقہ کار کی کامیابی کا انحصار مناسب پالیسی پیش رفت اور کنٹرول پر ہوتا ہے، ایک مؤثر مجاز طریقہ کار، استعمال میں آسان، بھروسہ مند کارگردگی، بتدریج گروتھ اور دیگر سسٹم سے اشتراک کے سبب صارفین کے ذریعہ قابل قبول ہوگا۔

(د) مجاز الکٹرانک ٹرانزکشن میں یکساں کوڈ اور جس کے کام نہ کرنے کے سبب قانونی خطرہ پیدا ہو سکتا ہے۔ حساس ٹرانزکشن مثلاً فنڈ کی منتقلی میں بینکوں کو دو فیکٹر مجازیت کے تحت یوزر آئی ڈی/ پاسورڈ اشتراک اور دوسرے فیکٹر جیسے (الف) ڈیجیٹل دستخط (کارپوریٹ صارف کے معاملہ میں ایک ٹوکن کے ذریعہ ڈیجٹل سرٹیفکیٹ اور یوسی اینڈ نجی کی حاصل کرنا ہوگا) یا (ب) ایک وقت کا پاسورڈ (او ٹی پی) ڈائنمک ایس کوڈ مختلف موڈس کے ذریعہ (مثلاً موبائل فون پر ایس ایم ایس بارڈ ہارڈ ویئر ٹوکن کے ذریعہ)

(ذ) آن لائن سیکورٹی مرحلہ، دوسرے چینل کی پیش رفت (مثلاً ٹیلی فون، ایس ایم ایس ای میل وغیرہ) کا استعمال پری سٹ ویلو کے ٹرانزکشن، نئے اکاونٹ کی لنکنگ تیار کرنے، تیسری پارٹی کی ادائیگی تفصیل کے رجسٹریشن، اکاونٹ تفصیل کی تبدیلی یا فنڈ منتقلی کی حد میں تبدیل میں کیا جا سکتا ہے، ان تبدیلی سیکورٹی متبادل کو اختیار کرنے کے لئے بینک اپنی اثر پزیری اور صارف ترجمات میں کثیر جہتی اضافی آن لائن سیکورٹی کے ذریعہ کر سکتے ہیں۔

(ر) باہمی مجاز پروٹوکول کی بنیاد پر صارفین بینک کی ویب سائٹ کی مجازیت کی جانچ سیکورٹی مکینزم کے ذریعہ مثلاً ذاتی یقین دہانی پیغامات

میسجز، سیکورٹی کوڈ کے تبادلے اور، یا ساکٹ لیئر تحفظ (ایس ایس ایل) سرور سرٹفکیٹ جانچ کر سکتے ہیں، حالیہ وقتوں میں ویلی ڈیشن سیکور ساکٹس لیئر (ای وی ایس ایس ایل) سرٹفکیٹ کا استعمال زیادہ کیا جارہا ہے کچھ خصوصی ایس ایس ایل سرٹفکیٹ ہوتے ہیں جو اعلیٰ سیکورٹی ویب بردورس کے ساتھ کام کر کے ویب سائٹ کی ادارہ جاتی شناحت کر سکتے ہیں اس بات کو اگر چہ ذہن نشین رکھنا چاہئے کہ ایس ایس ایل نٹ ورک ٹرانپورٹ لیئر میں ٹرانزٹ کے لئے ڈاٹا کوڈ میں تبدیلی کا کام کرتا ہے یہ ایپلکیشن لیئر میں ڈاٹا کے کوڈ میں منتقلی کی حتمی سیکورٹی میں فراہم کراتا ہے۔

(ز) ایک مجاز مشین کوڈ منتقلی پروٹوکول کے ساتھ صارفین سے باہمی مذکرات کے ذریعہ وابستہ ہوسکتا ہے مداخلت کے معاملہ میں ٹرانزکشن منسوخ بھی ہوسکتا ہے اور جس کے سبب ٹرانزکشن کا حل نکل سکتا ہے یا وائرس ہوسکتا ہے۔ ایسے معاملہ میں صارفین کو اس طرح کے واقعات کی اطلاع نوٹس کے ذریعہ یا ای۔میل، یا فون کے ذریعہ یا دیگر ذرائع سے دی جانا چاہئے۔

(س) موبائل فون میں تبدیلی صرف ایک بینک شاخ کے ذریعہ گذارش پر کی جاسکتی ہے۔

(ش) ورچوول کی بورڈ کا نفاذ ہونا چاہئے۔

(ص) جب نئے صارف شامل ہوں تو ایس ایم ایس/ای میل الرٹ کے بارے میں بتانا چاہئے۔

(ض) صارفین کو صلاح دی جاتی ہے کہ وہ مختلف حفاظتی تدابیر اختیار کریں اور اپنے ذاتی کمپیوٹر کو محفوظ رکھنے میں ان کا استعمال کریں اور عوامی یا انٹرنیٹ کیفے کمپیوٹر سے مالی ٹرانزکشن سے گریز کریں۔

(ط) خطرات پر منحصر ٹرانزکشن کی نگرانی یا سرویلانس مراحل کی ضرورت تو اضافی حصہ ہوگی۔

(ظ) آن لائن سیشن کے معاملہ میں ایک فیکسڈ مدت کے بعد اسے خود بخود ختم ہوجانا چاہئے۔ ورنہ صارف کو نئے سیشن کے لئے دوبارہ مجاز لینا پڑے گا، اس تبدیلی سے بینکنگ سیشن بلاشبہ حملہ آور سے محفوظ رہے گا۔

(ع) بطور تعریف ایک حقیقی کثیر جہتی فیکٹر کے مجاز ہونے کے لئے دو یا تین سے زائد فیکٹر زمرہ کی ضرورت کثیر جہتی سالوشن کا اسی زمرہ میں مختلف نکات سے استعمال پر سیکورٹی کا ہوگا یا دیگر بھرپائی کنٹرول رسائی کا حصہ ہوگا، لیکن یہ حقیقی کثیر جہتی فیکٹر مجازیت کو قائم نہیں کرسکتا۔

(غ) دو فیکٹر مجازیت کے انٹیگرل حصہ کے طور پر آرکے ٹکچر بینک مڈل مین کے حملوں کو کم کرنے کے لئے حفاظتی تدابیر اختیار کر سکتے ہیں جس کو عام طور پر مڈل اٹیک مین (ایم آئی ٹی ایم) بروسر مین (ایم آئی ٹی ٹی) اٹیک یا مین ان دی بروزر (ایم آئی ٹی جی) ایپلکیشن اٹیک کے طور پر جانتے ہیں۔

(ف) درمیانی حملہ آور شخص کے حملوں کو کم کرنے کے لئے بینک مندرجہ ذیل سیکورٹی بندوبست کر سکتے ہیں۔

(i) نئے پے ای کو جوڑنے کے لئے مخصوص اوٹی پی، ہر ایک نئے پے ای کو صارف منحصر اوٹی پی سے مجازیت حاصل کرنا ہوگا اور سکنڈ جینل سے پے ای کو تفصیل حاصل کرنا ہوگی یا صارف کے ہاتھ سے تحریر کردہ دستخط کو جو مینول طریقہ کار کا حصہ ہے بینک کو تصدیق کرنا ہوگا۔

(ii) ویلوٹرانزکشن کے لئے تنہا اوٹی پی (ادائیگی اور فنڈ کی منتقلی) ہر ایک ویلوٹرانزکشن یا ویلوٹرانزکشن کی تسلیم شدہ فہرست جس کا تعین صارف کے ذریعہ کیا جائے، کے لئے نئی اوٹی پی کی ضرورت درکار ہوگی۔

(iii) اوٹی پی ٹائم ونڈو: چینل پر منحصر اور وقت پر منحصر اوٹی پی مضبوط سیکورٹی فراہم کراتی ہے کیونکہ اسکی مجاز ہونے کی مدت بینک کے ذریعہ کنٹرول کی جاتی ہے اور اس کا انحصار استعمال کرنے والے کے طریقہ کار پر نہیں ہوتا، یہ سفارش کی جاتی ہے کہ بینکوں اوٹی پی ٹائم ونڈو کو ۳۰۰ اسکنڈز سے تجاوز کرنے کی اجازت سرور ٹائم سے زائد کی نہیں دینا چاہئے۔ اگر وہ ٹائٹ ونڈو سے چھوٹا ہے ایسا کرنے سے اوٹی پی کے غلط استعمال کا خطرہ کم ہوگا۔

(iv) ادائیگی اور فنڈ ٹرانسفر سیکورٹی: ڈیجیٹل دستخط اور اس کی منحصر میسیج مجاز کوڈس (کے ایم اے سی) ادائیگی کے لئے یا فنڈ ٹرانسفر ٹرانزکشن کے

لئے غیر مجاز موڈیفکشن کی جانچ یا ٹرانزکشن ڈاٹا میں مڈل مین کے اٹیک کا پتہ لگائے گا، اس سیکورٹی حل سے کام موثر طور پر ہوگا، ایک صارف جو ہارڈ ویئر ٹوکن استعمال کرتا ہے اسے ڈیجیٹل دستخط سے ٹرانزکشن کے لئے ون ٹائم پاس ورڈ جنریٹ کرنے کی ضرورت ہوگی ڈیجیٹل دستخط اس کے لئے بامعنی ہوگا ،جس کا مطلب ہوگا کہ ٹوکن سے لئے پے ای کا اکاونٹ نمبر اور ادا کی گئی رقم معلوم ہوگی جس سے ڈیجیٹل دستخط تیار کرنے کے لئے رقم حاصل کی جاسکے گی، مختلف اقسام کی پراسرار کلید او ٹی پی جنریٹ کرنے اور ٹرانزکشن کی سائننگ کے لئے دفع کی جاسکیں گی۔

(v) انٹرنٹ بینکنگ تناظر میں بینکوں کے لئے بہت کم موقع ہے کہ صارفین کے لئے ادائیگی روکنے کے لئے عمل کرسکیں اگر چہ بینک واضع طور پر صارفین کو مطلع کرسکتے ہیں اس مقررہ وقت اور حالات میں کوئی بھی اسٹاپ پیمنٹ منظور کیا جاسکے گا۔

(vi) صارف پروٹکشن ایکٹ 1986 میں ہندوستان میں صارفین کے حقوق کی وضاحت کی گئی ہے جو کہ بینکنگ خدمات پر نافذ ہے، وہ صارفین جو انٹرنٹ بینکنگ خدمات سے استفادہ کررہے ہیں ان کے حقوق اور ذمہ داریاں کیا ہیں اس کی صاف طور پر وضاحت کی گئی ہے، روایتی بینکنگ میں صارفین جن حقوق کا فائدہ اٹھاتے تھے، غیر مجاز ٹرانسفر بذریعہ ہیکنگ ،تکنیکی خامی کے معاملات میں صارفین کی نہیں بینکوں کی ذمہ داری کے تناظر میں بینکوں کو یہ یقینی بنانا ہوگا انٹرنٹ بینکنگ کی فراہمی میں وہ اس طرح کے خطرات کا کیسے مقابلہ کریں گے۔

(vii) بینکوں کی ویب سائٹ سے باہر لنک کی صورت میں اکثر وقار کا خطرہ پیدا ہوجاتا ہے اس طرح کے لنک صارفین کو اس بات کے لئے گمراہ نہیں کرسکتے کہ بینک کسی خاص پروڈکٹ کو اسپانسر کررہے ہیں یا کسی بزنس کا بینکنگ سے کوئی رشتہ نہیں ہے۔ بینکنگ ویب سائٹ سے باہر لنک کی صورت میں انہیں پورٹل پر بھروسہ کرنا چاہئے جنہوں نے پیمنٹ کا معاہدہ کیا ہو، دوسرے پورٹلوں سے بینک ویب سائٹ کے باہر لنک کا عمومی مطلب ہوتا ہے بینک صارفین کے ذریعہ پورٹل میں خرید سے متعلق اطلاع فراہم کرائی جائے ،بینکوں کو منظور کئے گئے نئے سیکورٹی احتیاط پر عمل کرنا ہوگا جب صارفین سے متعلق دیگر ویب سائٹوں سے خریدار کی گذارش پر عمل کیا جائے۔

(viii) سکنڈ چینل نوٹفیکشن/منظوری: بینک صارف کو سکنڈ چینل کے ذریعہ نوٹی فائی کریں گے سبھی ادائیگی یا فنڈ ٹرانزکشن میں مذکورہ بالا مخصوص ویلو جس کا تعین صارف کے ذریعہ کیا گیا ہو۔

(ix) ایس ایس ایل سرور سرٹفکیٹ انتباہ: انٹرنٹ بیکنگ صارفین کو یہ جاننا ہوگا کہ وہ کس طرح ایس ایس ایل یا ای وی، ایس ایس ایل سرٹفکیٹ انتباہ کا جواب دیں۔

(x) بینکوں کو خطرات پر منحصر ٹرانزکشن کی نگرانی اور سرویلانس مراحل پر عمل کرنا ہوگا، سافٹ ویئر میں صارف ٹرانزکشن طریقہ کار اور غیر مسلسل ٹرانزکشن کو روکنا یا آوٹ لائر ٹرازکشن کے لئے صارفین سے پیشگی معلومات حاصل کرنے کے لئے اشتراک پر عمل کرنا ہوگا۔