**<u>సైబర్ సంఘటనలను రిపోర్ట్ చేయడానికి అవసరమైన టెంప్లేట్</u>**

**1. RBIకు సెక్యూరిటీ సంఘటన రిపోర్టింగ్ (SIR) (2 నుంచి 6 గంటలలోపు)**

**2. RBIకు తదనంతర అప్‌డేట్స్ (గత రిపోర్టింగ్ అసంపూర్తిగా ఉంటే అంటే ఇన్వెస్టిగేషన్ జరుగుతూ ఉంటే లేదా ఆ సంఘటనకు సంబంధించి కొత్త సమాచారం ఏమైనా తెలిస్తే లేదా RBI విజ్ఞప్తి మేరకు) అప్‌డేట్ ఇవ్వాలి.**

**ప్రాథమిక సమాచారం**

**1. రిపోర్టింగ్ వివరాలు**

* బ్యాంకు పేరు

* RBI, CERT-In, ఇరత సంస్థలకు
రిపోర్టింగ్ చేసే తేదీ, సమయం
(రిపోర్టింగ్ చేసే సమయంలో ప్రతి ఒక్కరికీ
వేర్వేరుగా సమయాన్ని పేర్కొనండి)

* రిపోర్ట్ చేస్తున్న వ్యక్తి పేరు

* హోదా/విభాగం

*కాంటాక్ట్ వివరాలు (ఉదా. అధికారిక
ఈమెయిల్ ఐడీ, టెలిఫోన్ నెంబర్,
మొబైల్ నెంబర్ మొద.)

**2. సంఘటన వివరాలు**

* సంఘటనను గుర్తించిన తేదీ, సమయం

* సంఘటనల రకాలు, ప్రభావితమైన సిస్టమ్స్

(i) **క్రిటికల్ ఐటీ సిస్టమ్స్ ఔటేజ్**

(ఉదా. CBS, ట్రెజరీ సిస్టమ్స్, ట్రేడ్ ఫైనాన్స్ సిస్టమ్స్, ఇంటర్నెట్ బ్యాంకింగ్ సిస్టమ్స్, ATMలు, SWIFT, RTGS, NEFT, NACH, IMPS లాంటి పేమెంట్ వ్యవస్థలు)

(ii) **సైబర్ సెక్యూరిటీ సంఘటన**

(ఉదా. DDOS, రాన్సమ్ వేర్/క్రిప్టోవేర్, డాటా బ్రీచ్, డాటా డిస్ట్రక్షన్, వెబ్ డిఫేస్‌మెంట్ మొద.) (దయచేసి అనుబంధాన్ని పూర్తి చేయండి)

(iii) **సమచార సంగ్రహం లేదా మాయం కావడం** (ఉదా. కస్టమర్ లేదా బిజినెస్‌కు చెందిన ముఖ్యమైన సమాచారం మాయం కావడం లేదా నాశనం లేదా కరప్ట్ కావడం)

(iv) **ఇన్‌ఫ్రాస్ట్రక్చర్ అందుబాటులో లేకుండా పోవడం** (ఉదా: డీసీ/సెంట్రల్ ప్రాసెసింగ్ యూనిట్లు, శాఖ మొద., పవర్/యుటిలిటీ సప్లై, టెలీకమ్యూనికేషన్ సప్లై)

(v) **ఆర్థికం** ( ఉదా: లిక్విడిటీ, బ్యాంక్ రన్)?

(vi) **సిబ్బంది అందుబాటులో లేకపోవడం**

(ఉదా: ఎంత మంది, ఎంత శాతం సిబ్బంది

తక్కువగా ఉన్నారు/పని నుంచి ఆబ్సెంట్ అయ్యారు? )

(vii) **ఇతరములు** (ఉదా: ఔట్ సోర్స్‌డ్

సర్వీస్ ప్రొవైడర్లు, బిజినెస్ పార్ట్‌నర్లు,

ఐటీ చట్టం/ఇతర ఏవైనా చట్టాలు,

RBI/SEBI రెగ్యులేషన్ల ఉల్లంఘన మొద) ?

**3. ప్రభావాన్ని అంచనా వేయడం (ఉదాహరణలు ఇవ్వడం జరిగింది కానీ అవి పూర్తిగా కాదు)**

- సేవల అందుబాటుతో పాటు వ్యాపారంపై ప్రభావం - బ్యాంకింగ్ సేవలు, ఇంటర్నెట్ బ్యాంకింగ్, క్యాష్ మేనేజ్‌మెంట్, ట్రేడ్ ఫైనాన్స్, శాఖలు, ATMలు, క్లియరింగ్ మరియు సెటిల్‌మెంట్ కార్యకలాపాలు మొద.
- భాగస్వాములపై ప్రభావం - ప్రభావితమైన రిటైల్/కార్పోరేట్ కస్టమర్లు, ఆపరేటర్లు, సెటిల్‌మెంట్ సంస్థ(లు), బిజినెస్ పార్ట్‌నర్‌లు, సర్వీస్ ప్రొవైడర్లు మొద. ప్రభావితులైన భాగస్వాములు
- ఫైనాన్షియల్ మరియు మార్కెట్‌పై ప్రభావం – ట్రేడింగ్ కార్యకలాపాలపై ప్రభావం, ట్రాన్సాక్షన్ పరిమాణాలు, విలువలు, సొమ్ము నష్టం, లిక్విడిటీ ప్రభావం, బ్యాంక్ రన్, ఫండ్‌లను విత్‌డ్రా చేసుకోవడం మొద.
- రెగ్యులేటరీ మరియు చట్టాల ప్రభావం

**4. ఆయా సంఘటనల కాలక్రమానుగతం:**

- సంఘటన జరిగిన తేదీ, సమయం

  ఎంత కాలం పాటు?
- ఆ సంఘటన తీవ్రతను తగ్గించడానికి

  తీసుకున్న మధ్యంతర చర్యల కోసం

  తీసుకున్న అప్రూవల్‌లు, అలాంటి చర్యలు

  తీసుకోవడానికి గల కారణాలు
- సమాచారం ఇచ్చిన లేదా సంబంధం

  కలిగిన భాగస్వాములు
- ఉపయోగించిన కమ్యూనికేషన్ ఛానెల్స్

  (ఉదా: ఈమెయిల్, ఇంటర్నెట్, ఎస్సెమ్మెస్,

  ప్రెస్ రిలీజ్, వెబ్‌సైట్ నోటీస్ మొద.)
- BCP మరియు/లేదా DR నిర్ణయం/

  యాక్టివేషన్ చేయడానికి గల కారణాలు

5. మూల కారణ సమీక్ష (RCA)

- ఆ సమస్య ఎందువల్ల పుట్టింది/ఆ సంఘటన

  జరగడానికి కారణాలు, వాటి ప్రభావం.
- ఈ సమస్య పరిష్కారం/

  తీవ్రత తగ్గించేందుకు తీసుకున్న చర్యలు,

  ఆ చర్యలు తీసుకోవడానికి గల కారణాలు.
- దీర్ఘకాలంలో ఆ సమస్యను పరిష్కరించడానికి

  గుర్తించిన లేదా తీసుకున్న నివారణ

చర్యలు/ కరెక్షన్ల (ఒక్కసారి మాత్రమే) జాబితా

మరియు/లేదా అలాంటి సంఘటనలు

మళ్లీ భవిష్యత్తులో జరగకుండా

తీసుకున్న నివారణ చర్యలు

**6. తేదీ/సమస్య పరిష్కారానికి నిర్దేశించుకున్న లక్ష్యం……**

(DDMMYYYY)

-
-
-

---

గమనిక: వేరే విధంగా పేర్కొంటే తప్ప, అన్ని గళ్లనూ పూర్తి చేయాలి

# <u>సైబర్ సెక్యూరిటీ ఇన్సిడెంట్ రిపోర్టింగ్ (CSIR) ఫామ్</u>

**సాధారణ సమాచారం** **రిపోర్ట్ నెం:**

1. కాంటాక్ట్ సమాచారం: (పైన పేర్కొన్న ప్రాథమిక సమాచారంలో ఉన్నదానికన్నా వేరేగా ఉంటే పేర్కొనండి)

బ్యాంక్ పేరు:

రిపోర్ట్ చేస్తున్న వ్యక్తి పేరు, హోదా:

విభాగం:

అధికారిక ఈమెయిల్:

టెలిఫోన్/మొబైల్:

2. ఇది ఒక కొత్త సంఘటనా? ☐ లేదా ఇప్పటికే రిపోర్ట్ చేసిన సంఘటనకు అప్ డేటా? ☐

* దయచేసి మొదటి అప్ డేట్ కు 1 ని సూచించండి. ఒకవేళ ఇది ఇప్పటికే జరిగిన సంఘటనకు అప్ డేట్ అయితే, ఈ అప్‌డేట్‌కు అప్‌డేట్ సంఖ్యను ఇవ్వండి. (X1, X2, X3 , X4 మొదలైనవి. ఇక్కడ X అంటే రిపోర్ట్ సంఖ్య.

అప్‌డేట్ సంఖ్య: టెక్స్టను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

3. తీవ్రతను బట్టి ఈ సంఘటనను దేని కింద వర్గీకరించబడింది?

| | |
|---|---|
| తీవ్రత 1 ☐ | తీవ్రత 2 ☐ |
| క్రిటికల్ సిస్టమ్స్ ప్రభావితం/కస్టమర్ అప్లికేషన్ లేదా సిస్టమ్స్ సమస్యలను ఎదుర్కొంటున్నాడు. అంతర్గత నెట్‌వర్క్ దెబ్బ తినింది. లేదా వీటన్నిటి కలయిక. | సంఘటన బ్యాంక్ నెట్‌వర్క్/ క్రిటికల్ సిస్టమ్స్‌ను దెబ్బ తీసేంత తీవ్రం లేదా ఆ రెండింటి కలయిక |

**సంఘటన గురించి సమాచారం**

4. RBIకు ఈ సంఘటన గురించి సమాచారం అందించిన తేదీ, సమయం సూచించండి. ఇతర సంస్థలు, (CERT-In, NCIIP), చట్ట అమలు సంస్థలకు కూడా దీని గురించి వెల్లడించినట్లయితే, ఆ తేదీ, సమయం కూడా సూచించండి.

(దయచేసి భారతీయ స్థానిక కాలమానంలో సూచించండి (+ 5.30 GMT))

RBIకి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

CERT-In కి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

NCIIPకి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

.........కు రిపోర్ట్ చేసినది- సంస్థ పేరును పేర్కొనండి - తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

**5.ఎలాంటి విపత్తు/సంఘటన**

(దయచేసి ఒకటికన్నా ఎక్కువ ఎంపిక చేయండి, అవసరమైతే)

☐ డెనియల్ ఆఫ్ సర్వీస్

☐ డిస్ట్రిబ్యూటెడ్ డెనియల్ ఆఫ్ సర్వీస్

☐ వైరస్/వామ్/ట్రోజన్/మాల్‌వేర్

☐ ఇంట్రూజన్/హ్యాక్/అనధరైజ్డ్ యాక్సెస్

వెబ్‌సైట్ డిఫేస్‌మెంట్

సిస్టమ్స్‌ను దుర్వినియోగం/ఇతర అవసరాలకు ఉపయోగించుకోవడం

☐ APT ఏపీటీ/జీరో డే అటాక్

☐ స్పియర్ ఫిషింగ్/వేలింగ్/ఫిషింగ్/విషింగ్/సోషల్ ఇంజనీరింగ్ అటాక్

☐ ఇతరములు: టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

6. ఈ సంఘటనకు, గతంలో జరిగిన సంఘటనలతో సంబంధం ఉందా?

ఒక దానిని ఎంచుకోండి:

- అవును అయితే, ఈ రెండు సంఘటనలూ ఎలా సంబంధాన్ని కలిగి ఉన్నాయో మరింత సమాచారాన్ని ఇవ్వండి

టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

- గతంలో రిపోర్ట్ చేసిన సంఘటన రెఫరెన్స్‌ను పేర్కొనండి.

టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

**సంఘటన వివరాలు**

7. సంఘటన వివరాలను ఈ క్రింది బాక్స్‌లో ఇవ్వండి.

- ఈ మొదటి సంఘటనను ఎప్పుడు కనుగొన్నారు/గుర్తించారు/చూశారు?

తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

- ఈ సంఘటనను ఎలా కనుగొన్నారు/గుర్తించారు/చూశారు?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

* ఎవరు గుర్తించారు?

8. ఈ సంఘటన వల్ల ప్రభావితమైన క్రిటికల్ సిస్టమ్స్ లేదా నెట్‌వర్క్ ల వివరాలు ఇవ్వండి. దానిలో కనీసం ఈ క్రింది వివరాలు ఉండాలి:

ప్రదేశం, ఈ సిస్టమ్/నెట్‌వర్క్ పని, సిస్టమ్/నెట్‌వర్క్ లో నడుస్తున్న ప్రభావితమైన అప్లికేషన్లు( హార్డ్ వేర్ తయారీదారు, సాఫ్ట్ వేర్ డెవలపర్, మేక్/మోడల్ మొద) మొద.

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

ప్రస్తుతం సిస్టమ్‌లో ఎలాంటి సెక్యూరిటీ సాఫ్ట్ వేర్ ఇన్ స్టాల్ చేయబడి ఉంది?

ఈ సంఘటనలో ప్రమేయమున్న ఏవైనా TCP లేదా UDP పోర్టుల వివరాలు, ఒకవేళ తెలిసింటే.

ప్రభావితమైన సిస్టమ్ IP అడ్రస్, ఒకవేళ తెలిసి ఉంటే. ఒకవేళ తెలిస్తే అటాక్ చేసిన వారి IP అడ్రస్‌ను పేర్కొనండి.

అవసరం అనిపించన చోట, దయచేసి ప్రభావితమైన క్రిటికల్ సిస్టమ్ యొక్క OSను పేర్కొనండి: ఏదైనా ఒక దానిని ఎంచుకోండి :

- ఇతరములు అయినట్లయితే, OS పేరును పేర్కొనండి. :

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

9. ఆ దాడి యొక్క ప్రభావం ఏమిటి? (ప్రతి కాలమ్ కు ఒక బాక్స్‌లో టిక్ పెట్టండి)

| కస్టమర్ సర్వీస్ డెలివరీ | సెన్సిటివ్ సమాచారం (నష్టం) | ప్రజల విశ్వాసం, సంస్థ ప్రతిష్ఠ |
|---|---|---|
| ☐ ఎలాంటి ప్రభావం లేదు | ☐ ఎలాంటి నష్టమూ లేదు | ☐ ఎలాంటి ప్రభావం లేదు |
| ☐ తక్కువ ప్రభావం | ☐ తక్కువ నష్టం | ☐ తక్కువ ప్రభావం |
| ☐ ఎక్కువ ప్రభావం | ☐ ఎక్కువ నష్టం | ☐ ఎక్కువ ప్రభావం |
| ☐ తీవ్రమైన ప్రభావం | ☐ తీవ్రమైన నష్టం | ☐ తీవ్రమైన ప్రభావం |
| ☐ భారీ ప్రభావం | ☐ భారీ నష్టం | ☐ భారీ ప్రభావం |

10. ప్రభావితమైన క్రిటికల్ సిస్టమ్స్/ నెట్ వర్కులు బ్యాంకు యొక్క ఇతర క్రిటికల్ సిస్టమ్స్/ క్రిటికల్ అసెట్స్ పై ప్రభావం చూపే అవకాశముందా?

ఒక దానిని ఎంచుకోండి :

అవును అయితే, మరిన్ని వివరాలు తెలియజేయండి.

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

**సంఘటన స్థితి**

11. ఆ సమయంలో తీసుకున్న ఫాలో అప్ చర్యలు ఏమి?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

12. ప్రస్తుత పరిస్థితి లేదా ఈ సంఘటన అనంతర తీర్మానాలేమి?

ఒక దానిని ఎంచుకోండి:

ఒకవేళ అది పరిష్కారం కానట్లయతే, తర్వాత కార్యాచరణ ఏమిటి?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

13. మీకు తెలిసి దాడి జరిగిన/కాంప్రమైజ్ అయిన మొదటి తేదీ ? (తెలియకుంటే చెక్ బాక్స్‌లో టిక్ చేయండి)

(దయచేసి భారతీయ స్థానిక కాలమానంలో సూచించండి (+ 5.30 GMT))

తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి. తెలియదు : ☐

14. ఈ సంఘటనకు మూలం/కారణం ఏమిటి? (నిల్ లేదా తెలియకపోతే ఎన్ి )

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

15. ఈ సంఘటనను CERT-In, NCIIP/ఏదైనా చట్ట అమలు సంస్థ/ IBCARTకు రిపోర్ట్ చేయడం జరిగిందా? ఒక దానిని ఎంచుకోండి.

* అవును అయితే , రిపోర్ట్ చేసిన ఏజెన్సీని పేర్కొనండి.

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

16. చెయిన్ ఆఫ్ కస్టడీని మెయిన్ టెయిన్ చేస్తున్నారా?

17. బ్యాంక్ చెయిన్ ఆఫ్ కస్టడీ ఫామ్‌ను నింపుతోందా?

18. ఈ సంఘటన అనంతరం సాక్ష్యాలను నమోదు చేయడానికి ఏ టూల్స్‌ను ఉపయోగించడం జరిగింది?

**అటాక్ వెక్టర్స్**

E1. బ్యాంకు ఈ సంఘటనకు సంబంధించిన IP అడ్రస్ లు, డొమైన్ పేర్లు గుర్తించిందా?

ఇండికేటర్స్ ఆఫ్ కాంప్రమైజ్, సంఘటనలో గుర్తించిన IP అడ్రస్‌లు, సంఘటనలో ప్రమేయం కలిగిన IP అడ్రస్‌లు (బాధితులు, మాల్ వేర్ కమాండ్ అండ్ కంట్రోల్ సర్వర్లు మొద.), పరిష్కరించిన డొమైన్ నేమ్స్, సంఘటనలో ప్రమేయం కలిగిన డొమైన్ నేమ్స్ (ఉదా: డ్రైవ్ బై డౌన్ లోడ్ సర్వర్లు, మాల్ వేర్ కంట్రోల్ అండ్ కమాండ్ సర్వర్లు, డీ ఫేస్డ్ వెబ్ సైట్లు), గుర్తించిన ఈమెయిల్ అడ్రస్‌లు వాటి ప్రమేయం, హానికారక ఫైల్స్/అటాచ్‌మెంట్స్ (ఫైల్ పేరు, సైజు, MD5/ IPSHA 1 హ్యాష్ మొద) మొదలైన వాటి గురించి IBCART, CERT-In, చట్టాన్ని అమలు చేసే సంస్థలకు రిపోర్ట్ చేయడం జరిగిందా?