Template for reporting Cyber Incidents

1. **Security Incident Reporting (SIR) to RBI (within two to 6 hours):**
2. **Subsequent update(s) RBI (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI):**

Basic Information	
1. Particulars of Reporting:	
• Name of the bank	
• Date and Time of Reporting to RBI, CERT-IN, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident:	
• Date and time of incident detection	
• Type of incidents and systems affected (i) **Outage of Critical IT system(s)** (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.) (ii) **Cyber Security Incident** *(e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web*	

defacement, etc.)? ***[Please complete Annex]*** (iii) **Theft or Loss of Information** *(e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)?* (iv) **Outage of Infrastructure** *(e.g. which premises-DC/Central Processing Units, branch, etc., power/utilities supply, telecommunications supply,)?* (v) **Financial** *(e.g. liquidity, bank run)?* (vi) **Unavailability of Staff** (e.g. number and percentage on loss of staff /absence of staff from work (vii) **Others** *(e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/SEBI regulations. Etc.)?*	
• What actions or responses have been taken by the bank at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment(examples are given but not exhaustive):	
• Business impact including availability of services – Banking Services, Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	

• Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc.	
• Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc.	
• Regulatory and Legal impact	
4. Chronological order of events:	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	
• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such	

measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution_____ (DD/MM/YYYY).	
•	
•	
•	

Note: All fields are REQUIRED to be filled unless otherwise stated.

CYBER SECURITY INCIDENT REPORTING(CSIR) FORM	
General Information	**Report No:**

1. Contact Information: *(Please provide if different from what is reported in Basic Information above)*

Name of bank:

Name of the person reporting and Designation:

Department

Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

- For the first update, please indicate "1. If this is an update to a reported incident, please provide the update number for this update. (X.1, X.2, X.3, X.4, etc. where X is the Report No.
  Update No: Click here to enter text.

3 What severity is this incident being classified as?

Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the bank's network / critical system(s) or a combination of them at risk	

Information about the Incident

4. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-IN/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

(Please specify in Indian Local Time (+5.30 GMT))

Reported to RBI - Date: Click here to enter a date.

Reported to CERT-IN Date: Click here to enter a date.

Reported to NCIIP Date: Click here to enter a date.

Reported to ----mention the name of agency Date: Click here to enter a date.

5. Types of Threat/Incident

((Please select more than one, as applicable)

☐ Denial of Service (DoS) ☐ Distributed Denial of Service (DDoS)

☐ Virus/Worm/Trojan/Malware ☐ Intrusion/Hack/Unauthorised access

☐ Website Defacement ☐ Misuse of Systems/Inappropriate usage

☐ APT/0-day attack ☐ Spear phishing/Whaling/Phishing/Wishing/Social engineering attack

☐ Other: Click here to enter text.

6. Is this incident related to another incident previously reported?

Choose an item.

- If “Yes”, provide more information on how both incidents are related. Click here to enter text.
- Please provide the reference no. of the previously reported incident.

Ref no: Click here to enter text.

Incident Details

7. Please provide details of the incident in the box below.

- When was the incident first observed/sighted/detected?
  Click here to enter a date.

- How was the incident first observed/sighted/detected?
  Click here to enter text.

- Who observed?

8. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

-Location, purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.

Click here to enter text.

What security software installed on the system currently?

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's IP address

Where relevant, please indicate the Operating System of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

9. What is the impact of the attack? (*Tick 'one' checkbox for each column*)

Customer Service Delivery	(Loss of) Sensitive Information	Public Confidence and Reputation
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact

☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

10. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?

Choose an item.

- If "Yes", please provide more details.

Click here to enter text.

Incident Status

11. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

Click here to enter text.

12. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

13. What is the earliest known date of attack or compromise? *(Tick 'checkbox' if unknown)*

(Please specify in Indian Local Time +5.30 GMT)

Date: Click here to enter a date. Unknown: ☐

14. What is the source/cause of the incident? *('NIL' OR 'NA' if unknown)*

Click here to enter text.

15. Has the incident been reported to CERT-IN/NCIIP/ any law enforcement agency/IBCART? Choose an item.

- If "Yes", specify the agency that is being reported to.

Click here to enter text..

16. Is chain of custody maintained?

17. Has the bank filled chain of custody form?

18. What tools were used for collecting the evidence for the incident?

: Attack Vectors

E1. Did the bank locate/identify IP addresses**, domain names, related to the incident**

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/Law enforcement agencies
