

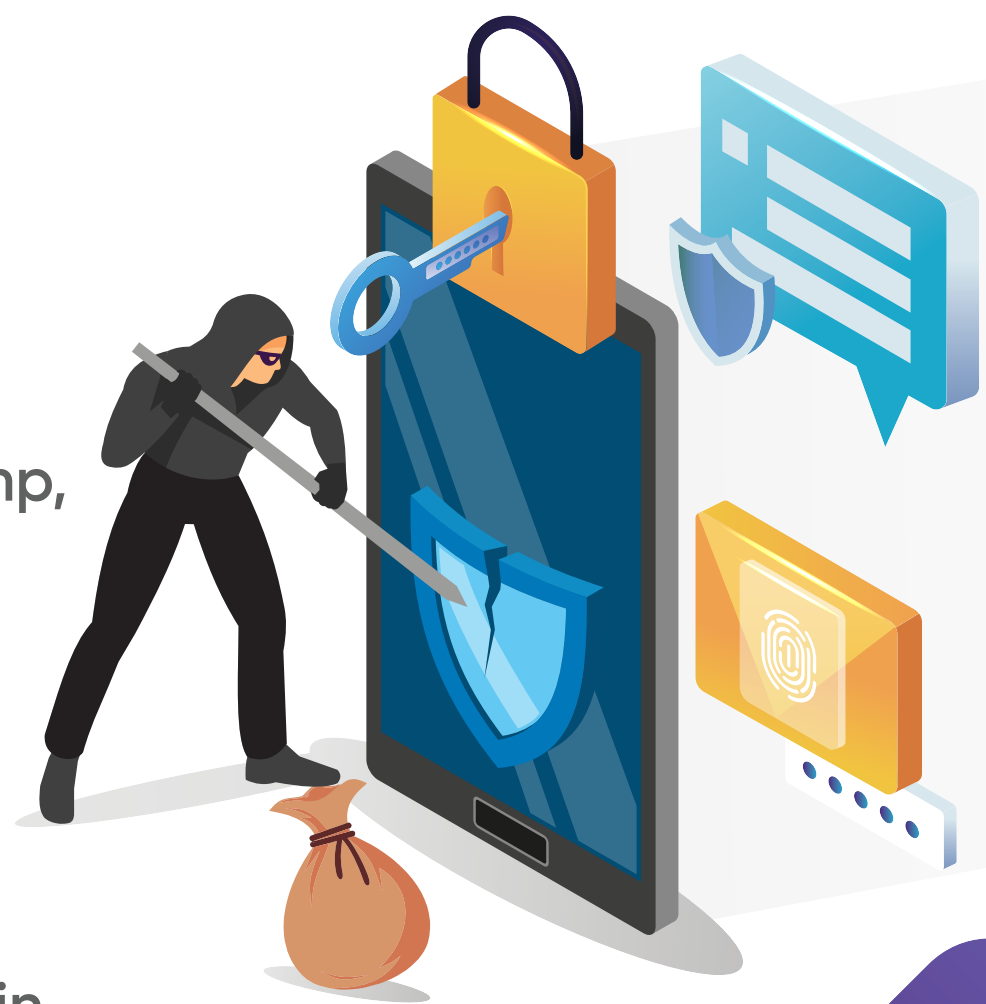
CERT-In: Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet

Summary of the Circular:

The directions issued to service providers, intermediaries, data centres, body corporate and government organisations cover synchronization of ICT system clocks, reporting of cyber incidents to CERT-In, types of cyber incidents to be reported, maintaining logs of ICT systems, registration of information about subscribers /customers and maintaining KYC records.

Key Pointers and Controls to be Implemented:

1. Synchronization of all ICT system clocks
 - a. Shall connect to NTP server of NIC or NPL
 - b. Time source shall not deviate from NPL and NIC
2. Cyber incidents shall be reported to CERT-In within 6 hours
 - a. CERT-In has provided a list of 20 cyber incidents
3. Point of Contact (POC) shall be assigned for communicating with CERT-In
4. All ICT system logs shall be securely stored for a rolling period of 180 days
5. Transaction Logs and Records including IP Address, timestamp, and time zone Transaction ID, accounts involved shall be securely stored
6. Logs shall be maintained within INDIAN JURISDICTION
7. Virtual Private Network and Server providers, Cloud Service Providers shall maintain customer/subscriber details for 5 Years after cancellation/withdrawal
8. Virtual Asset Service, Asset Exchange Providers shall maintain KYC data and financial transaction data for 5 Years



Action items for the applicable entities:

1. Plan to adhere to the directions within 60 days from the date of issue of the circular (Apr 28th, 2022)
2. Identify and Assign a POC for reporting and communicating with CERT-In
3. Review and Update the relevant information security policies of the organization to include and implement the directions of the circular
 - a. e.g. Incident Management, Logging Monitoring, Data Retention, Cyber Crisis Management Plan

Applicable:

1. All service providers, intermediaries, data centres, corporate bodies and Government Organizations including:
 - a. Virtual Private Server (VPS) Providers
 - b. Cloud Service Providers (CSPs)
 - c. Virtual Private Network Service (VPN Service) Providers
 - d. Virtual Asset Service Providers,
 - e. Virtual Asset Exchange Providers
 - f. Custodian Wallet Providers
2. Non-Indian entities providing service to Indian customers or operating out of India

