

No. 21(03)/2022-Pers./3144816
Government of India
Ministry of Electronics & Information Technology
National Informatics Centre
A-Block, CGO Complex, Lodhi Road, New Delhi-110003

Dated: 15th November, 2022

OFFICE MEMORANDUM

The undersigned is directed to refer to the directions issued by CERT-In vide communication No. 20(3)/2022-CERT-In dated 28 April, 2022 (https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf) and to say that the following directives need to be strictly adhered to by all individual concerned.

- (i) All cyber incidents (as mentioned in the Annexure) shall be mandatorily reported to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents.

The Incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). Details regarding methods and formats of reporting cyber security incidents (updated from time to time) are also published on the website of CERT-In (www.cert-in.org.in).

- (ii) All ICT systems shall mandatorily enable logs and maintain them securely for a rolling period of 180 days.

- (iii) All ICT systems shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) for time syhchronisation.

2. This issues with the approval of the Competent Authority.


(Manoharan R)
Joint Director (Pers.)
Ph. No. 24305442

Encl: As above

Copy to:

1. All officers/officials of NIC....through DigitalNIC
2. CISO, NIC Hqrs ... w.r.t. his note dated 10.11.2022 vide file No. M-13/1470/2022-NIC Hqr(3145304)
3. Staff Officer to DG, NIC ... for kind information
4. Vigilance Officer, NIC
5. Guard File/Personal File/DigitalNIC

-sd-
(Manoharan R)
Joint Director (Pers.)

Annexure**Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:**

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

- i. Targeted scanning/ probing of critical networks/ systems
- ii. Compromise of critical systems/ information
- iii. Unauthorised access of IT systems/ data
- iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- v. Malicious code attacks such as spreading of virus/ worm/ Trojan/ Bots/ Spyware/ Ransomware/ Cryptominers
- vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
- vii. Identity Theft, spoofing and phishing attacks
- viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- x. Attacks on Application such as E-Governance, E-Commerce etc.
- xi. Data Breach
- xii. Data Leak
- xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- xiv. Attacks or incident affecting Digital Payment systems
- xv. Attacks through Malicious mobile Apps
- xvi. Fake mobile Apps
- xvii. Unauthorised access to social media accounts
- xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/ software/ applications
- xix. Attacks or malicious/ suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
- xx. Attacks or malicious/ suspicious activities affecting systems/ servers/ software/ applications related to Artificial Intelligence and Machine Learning.
