

# DECODING THE CERT-IN DIRECTIVE FOR ENTERPRISES TO REPORT CYBER INCIDENTS







## Overview

Between January and June 2022, India reported a total of 670,000 cyber security [incidents](#). These attacks threaten the security of individuals and enterprises across the country.

To curb the rising number of cyber security breaches, the Indian government is driving several initiatives that enhance the cyber security posture and reporting of cyber incidents. In April 2022, the Indian Computer Emergency Response Team (CERT-In) made it a requirement that all cyberattacks be reported. Not only will this help organisations strengthen their cybersecurity posture, but it will also prevent losses and disruptions in services due to cyberattacks.

All organisations under the direct purview of the IT ACT 2000 will be part of this directive (sub-section (6) of section 70B), which became effective on September 25, 2022.

## Tata Communications recommendations to address CERT-In requirements

Task name	Task description	Recommendations to address CERT-In requirements	Organisation's compliance check list
 Synchronisation of all ICT system clocks with NTP	Ensure to connect to the Network Time Protocol (NTP) server of National Informatics Centre (NIC) or National Physical Laboratory (NPL)	<ul style="list-style-type: none"> <li>• Synchronisation with NIC or NPL</li> <li>• Global enterprises can pick any atomic server</li> </ul>	
 Designating a point of contact and maintaining records	Ensure a Point Of Contact for CERT-In interactions	<ul style="list-style-type: none"> <li>• Customer must designate the point of contact for interacting with CERT-In</li> <li>• CSIRT/IT Security Incident Manager is mandatory</li> </ul>	
 Reporting of incidents	Ensure reporting cyber security incidents to the Indian Computer Emergency Response Team (CERT-In) as per the methods and formats published on their website*	<ul style="list-style-type: none"> <li>• Security monitoring is essential to identify security incidents either through captive or outsourced Security Operations Center (SOC)</li> <li>• Customers are to report cyber security incidents to CERT-In within six hours</li> </ul>	
 Maintain Logs	<ul style="list-style-type: none"> <li>• Enable logs of all ICT systems and maintain them securely for a rolling period of 180 days</li> </ul> <p><b><u>Essential logs</u></b></p> <ul style="list-style-type: none"> <li>• FW, IPS, Web/DB/Mail/Proxy/FTP, APP</li> <li>• ATM Switch, IoT, SSH, VPN logs</li> </ul>	<ul style="list-style-type: none"> <li>• From the incident response and analysis perspective, both successful as well as unsuccessful events shall be recorded</li> </ul>	

Tata Communications, a CERT-In empaneled and award-winning cyber security vendor, delivers [cyber security](#) from the cloud to endpoints. Our comprehensive security capabilities prevent threats at the network edge with round-the-clock threat management, cloud security, and governance risk and compliance management services. Tata Communications helps enterprises achieve a proactive security posture by protecting them from internal and external threats.

Our platform-based SOC services have the capability of identifying advanced threats and storing logs for 365 days. Additionally, we can provide the necessary support to clients for extracting adequate security incident data during CERT-In notifications.

## Repercussion for non-compliance with CERT-In directions

Non-compliance with the CERT-In directions may result in imprisonment for a period of up to 1 year or a fine of up to INR 100,000 or both. However, in most cases, imprisonment is usually not resorted to in the first instance.

## Conclusion

The CERT-In directive provides guidance to enterprises to protect their IT infrastructure from increased cyber threats. Organisations must partner with cyber security providers that can protect the entire IT infrastructure, manage complex incident management, and simplify reporting.



Annexure I	Annexure II	Annexure III
<p>Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:</p> <p>[Refer Rule 12 (1) (a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]</p> <ul style="list-style-type: none"> <li>• Targeted scanning/probing of critical networks/systems</li> <li>• Unauthorised access of IT systems/data</li> <li>• Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Cryptominers</li> <li>• Identity Theft, spoofing and phishing attacks</li> <li>• Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks</li> <li>• Data Breach</li> <li>• Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers</li> <li>• Attacks through Malicious mobile Apps</li> <li>• Unauthorised access to social media accounts</li> <li>• 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</li> <li>• Compromise of critical systems/information</li> <li>• Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.</li> <li>• Attack on servers such as Database, Mail and DNS and network devices such as Routers</li> <li>• Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks</li> <li>• Attacks on Application such as E-Governance, E-Commerce etc.</li> <li>• Data Leak</li> <li>• Attacks or incident affecting Digital Payment systems</li> <li>• Fake mobile Apps</li> <li>• Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications</li> <li>• Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning</li> </ul> <p>The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In <a href="http://www.cert-in.org.in">www.cert-in.org.in</a> and will be updated from time to time.</p>	<p>Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In</p> <p>The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Designation</li> <li>• Organisation Name</li> <li>• Office Address</li> <li>• Email ID</li> <li>• Mobile No.</li> <li>• Office Phone</li> <li>• Office Fax</li> </ul>	<p>KYC Requirements For the purpose of KYC, any of following Officially Valid Document (OVD) as a measure of identification procedure prescribed by the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 / Securities and Exchange Board of India Clarification on Know Your Client (KYC) Process and Use of Technology for KYC vide Circular SEBI/HO/MIRSD/DOP/CIR/P/2020 /73 dated April 24, 2020 / The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Local and Outstation category customers, shall be used and maintained:</p> <ul style="list-style-type: none"> <li>• The passport</li> <li>• The driving license</li> <li>• Proof of possession of Aadhaar number</li> <li>• The Voter's Identity Card issued by the Election Commission of India</li> <li>• Job card issued by NREGA duly signed by an officer of the State Government and</li> <li>• Letter issued by the National Population Register containing details of name and address.</li> <li>• Validated phone number</li> <li>• Trading account number and details, Bank account number and bank details</li> </ul> <p>For the purpose of KYC for business entities (B2B), documents mentioned in the Customer Due Diligence (CDD) process prescribed in Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time shall be used and maintained.</p>

#### Sources:

[https://www.cert-in.org.in/PDF/CERT-In\\_Directions\\_70B\\_28.04.2022.pdf](https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf)  
[https://www.cert-in.org.in/PDF/FAQs\\_on\\_CyberSecurityDirections\\_May2022.pdf](https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf)  
[https://www.cert-in.org.in/PDF/CERT-In\\_directions\\_extension\\_MSMEs\\_and\\_validation\\_27.06.2022.pdf](https://www.cert-in.org.in/PDF/CERT-In_directions_extension_MSMEs_and_validation_27.06.2022.pdf)  
<https://www.idc.com/research/viewtoc.jsp?containerId=AP49574122>  
<https://www.csoonline.com/article/3663732/indian-cis-os-voice-concerns-on-cert-in-s-new-cybersecurity-directives.html>

\* Note: Reporting of cyber incidents (as mentioned in Annexure I of the Indian Computer Emergency Response Team (CERT-In )-No. 20(3)/2022- CERT.in)) to CERT-In is to be done within six hours of noticing such incidents

For more information, visit us at [www.tatacommunications.com](http://www.tatacommunications.com)

Schedule A Consultation



© 2022 Tata Communications. All Rights Reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Limited in certain countries.