October 31, 2026

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

CERT-In directions: logs, clocks, records and incident reports

CERT-In directions are six cyber security instructions the Indian Computer Emergency Response Team (CERT-In) issued on April 28, 2022. Covered businesses and government bodies must report listed incidents within 6 hours, sync clocks and keep logs for 180 days within Indian jurisdiction. Ignoring them risks up to one year in prison, a fine of up to ₹1 crore, or both.

CERT-IN'S DIRECTIONS are six numbered instructions, (i) to (vi), issued on April 28, 2022 under section 70B(6) of the Information Technology Act, 2000 (the IT Act). Section 70B(6) lets CERT-In call for information from, and give directions to, service providers, intermediaries, data centers, companies and any other person. The directions took effect 60 days after issue.

KEY FACTS

DATA PROTECTION

Digital Personal Data Protection Act, 2023

DATA RULES

Digital Personal Data Protection Rules, 2025

IT LAW

Information Technology Act, 2000

UPDATED

October 31, 2026

CERT-In directions: logs, clocks, records and incident reports

Ministry of Electronics and Information Technology · October 31, 2026

CERT-In directions are six cyber security instructions the Indian Computer Emergency Response Team (CERT-In) issued on April 28, 2022. Covered businesses and government bodies must report listed incidents within 6 hours, sync clocks and keep logs for 180 days within Indian jurisdiction. Ignoring them risks up to one year in prison, a fine of up to ₹1 crore, or both.

What are CERT-In's directions?

CERT-In's directions are six numbered instructions, (i) to (vi), issued on April 28, 2022 under section 70B(6) of the Information Technology Act, 2000 (the IT Act). Section 70B(6) lets CERT-In call for information from, and give directions to, service providers, intermediaries, data centers, companies and any other person. The directions took effect 60 days after issue.

The six directions of April 28, 2022 (No. 20(3)/2022-CERT-In)

Direction	What it asks
(i) Clocks	Sync the clocks of all information and communication technology (ICT) systems to the time servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or to servers traceable to them
(ii) Incident reports	Report the cyber incidents listed in Annexure I within 6 hours of noticing them or being told of them
(iii) Orders	Act, give information or help when CERT-In orders it, and name a Point of Contact
(iv) Logs	Keep logs of all ICT systems for a rolling 180 days, within Indian jurisdiction
(v) Customer records	Data centers and virtual private server (VPS), cloud and virtual private network (VPN) providers record seven customer details, for 5 years or longer if a law requires, after the registration ends
(vi) Virtual asset records	Virtual asset service providers, exchanges and custodian wallet providers keep know your customer (KYC) and transaction records for 5 years

The Indian Computer Emergency Response Team (CERT-In) is India's national agency for responding to cyber security incidents. The central government appointed it under section 70B(1) of the IT Act (CERT-In's FAQ, Q2).

Since October 12, 2026, CERT-In has worked as an attached office under the administrative control of MeitY, the Ministry of Electronics and Information Technology. It remains the agency appointed under the IT Act (MeitY's order of October 12, 2026, paras 1 and 2).

On October 31, 2026, CERT-In's page of section 70B directions still listed these as its only directions, beside their FAQ, the June 2022 extension and a vulnerability report form.

For the rest of MeitY's rules, see MeitY: India's data, platform, cyber security and electronics rules.

Who must follow the CERT-In directions?

Service providers, intermediaries, data centers, companies and other businesses, and government bodies must follow CERT-In's directions; individual citizens aren't covered. CERT-In's FAQ says a provider serving users in India names a Point of Contact even with no office in India. For micro, small and medium enterprises (MSMEs), the directions took effect on September 25, 2022.

- **Any entity, for incidents:** the directions apply to any entity in the matter of cyber incidents, CERT-In's FAQ says (Q26). It cites sections 1 and 75 of the IT Act.
- **Foreign providers:** service providers, intermediaries, data centers, companies and other businesses serving users in India name a Point of Contact, even with no physical presence in India (FAQ Q29).
- **MSMEs:** the directions took effect for them on September 25, 2022, under CERT-In's extension of June 27, 2022.

What must you report, and how fast?

You must report the cyber incidents listed in Annexure I of CERT-In's directions within 6 hours of noticing them or being told of them (direction (ii)). The 20 kinds include data breaches, ransomware, phishing and attacks on cloud and AI systems. CERT-In's FAQ says you may report what you know in 6 hours, the rest later within reasonable time (Q30).

Direction (iii) adds a second duty: when CERT-In orders it, you must act, give information or help within the time and in the format it sets.

For the full incident list and the data protection breach report, see Data breach reporting in India: CERT-In's 6 hours and DPDP's 72.

How long must you keep logs, and where?

Direction (iv) of CERT-In's directions says to enable logs of all your ICT systems and keep them securely for a rolling 180 days, within Indian jurisdiction. You give them to CERT-In with an incident report or when it orders you to. CERT-In's FAQ says a CERT-In officer of Deputy Secretary rank or above may ask for them (Q38).

CERT-In's FAQ reads differently: logs may also be stored outside India if you produce them to CERT-In in reasonable time (Q35). Yet it also says a provider serving users in India keeps them in Indian jurisdiction (Q36). The FAQ says it isn't a legal document; direction (iv) is the binding text.

India's data protection rules add a separate one-year duty. A Data Fiduciary decides why and how personal data is processed, under section 2(i) of the Digital Personal Data Protection Act, 2023 (the DPDP Act). Under the DPDP Rules, 2025, it keeps the logs and personal data needed to detect and investigate unauthorized access for one year, unless another law requires otherwise (rule 6(1)(e)).

Rule 8(3) adds a one-year minimum for personal data, traffic data and processing logs, for the purposes in the Rules' Seventh Schedule, at the Data Fiduciary's processors too. Both rules start at the eighteen-month step: about May 13, 2027 (eighteen months after the Gazette of November 13, 2025), under rule 1(4). CERT-In's 180 days apply now.

For the Indian rules that keep data or logs in India, see Cross-border data transfer under India's DPDP Act.

Must your clocks sync to Indian time servers?

Yes. Direction (i) says to connect all your ICT system clocks to the time servers of the National Informatics Centre (NIC) or the National Physical Laboratory (NPL), or to servers traceable to them. An entity whose ICT systems span several geographies may use another accurate, standard time source that doesn't deviate from NPL and NIC.

CERT-In's FAQ goes further: any organization may use another accurate, standard time source that conforms to NPL and NIC (Q40). Clocks needn't be set to Indian Standard Time, as long as

the time zone is recorded with the time (Q40). Customers who rely on a cloud's own time service may keep using it (Q42). NIC's time servers are samay1.nic.in and samay2.nic.in, and NPL's is time.nplindia.org (Q43).

What must data centers, cloud, VPS and VPN providers record?

Data centers and VPS, cloud and VPN providers must record validated customer names, hire periods, IP addresses, contacts, purpose and ownership. Under direction (v), they keep the records for 5 years, or longer if a law requires, after the registration is canceled or withdrawn.

Records and how long

Who	What they record	Kept for	Direction
Data centers, VPS, cloud and VPN providers	Validated names of customers; period of hire, with dates; IP addresses allotted or used; email address, IP address and time stamp at sign-up; purpose of hire; validated address and contact numbers; ownership pattern	5 years, or longer if a law requires, after the registration is canceled or withdrawn	Direction (v), items a to g
Virtual asset service providers, virtual asset exchanges and custodian wallet providers	All KYC information and records of financial transactions	5 years	Direction (vi)

CERT-In's extension of June 27, 2022 moved items a (validated names) and f (validated address and contact numbers) to September 25, 2022.

CERT-In's FAQ says the VPN rule doesn't cover enterprise or corporate VPNs, only entities offering internet proxy-like services to general internet users (Q34).

Direction (v) puts the record duty on the providers, not their customers. Individual citizens aren't covered by the directions at all (FAQ Q7).

Do you have to report vulnerabilities?

Under CERT-In's directions, no: its FAQ says reporting a vulnerability on its own, unconnected with an incident, isn't mandatory (Q15). But CERT-In's guidelines of June 10, 2026 ask equipment makers and technology providers to tell CERT-In and affected organizations immediately about critical and high-severity vulnerabilities in what they supply.

The guidelines on AI-accelerated vulnerability protection and response (CISG-2026-03, version 1.0) cover all global and domestic original equipment manufacturers (OEMs) and technology providers operating in India. They include software vendors, hardware makers, cloud and managed service providers, system integrators and digital service providers (section 1).

Critical vulnerabilities, scored 9.0 to 10.0 on the Common Vulnerability Scoring System (CVSS), and high ones, 7.0 to 8.9, should go to affected organizations and CERT-In "immediately upon discovery or confirmation" (section 2.1(b)). A zero-day vulnerability or active exploitation should also be reported to them, CERT-In included, immediately (section 2.1(c)).

Indicative patch timelines by severity (CERT-In guidelines of June 10, 2026, section 3.1). IT is information technology; OT is operational technology.

Severity (CVSS score)	Likely to be exploited using AI: IT / OT	Identified or reported through responsible disclosure: IT / OT
Critical (9.0 to 10.0)	Emergency release / 7 to 15 days	5 days / 15 to 30 days
High (7.0 to 8.9)	7 days / 15 to 30 days	15 days / 30 to 60 days
Medium (4.0 to 6.9)	14 days / 30 to 60 days	30 days / 60 to 90 days

CERT-In calls the text "guidelines / recommendations" (section 1), and its page of section 70B directions didn't list it on October 31, 2026. An incident on the Annexure I list, such as a data breach, still goes to CERT-In within 6 hours under direction (ii).

What is the penalty for not following CERT-In's directions?

The penalty for not following CERT-In's directions is up to one year in prison, a fine of up to ₹1 crore, or both (IT Act, section 70B(7)). The same applies to failing to give CERT-In information it calls for. The maximum fine was ₹1 lakh until the Jan Vishwas Act, 2023 raised it, from November 30, 2023.

CERT-In's FAQ of May 2022 still quotes the out-of-date fine of up to ₹1 lakh (introduction, para 4). That was the figure the Information Technology (Amendment) Act, 2008 wrote into section 70B(7).

The Jan Vishwas (Amendment of Provisions) Act, 2023 put "one crore" in place of "one lakh" (Schedule, serial 32, entry (I)). S.O. 4745(E) brought the change into force on November 30, 2023.

CERT-In says it will use the power reasonably, on occasions when non-compliance is deliberate (FAQ Q23).

For one sector's 2026 cyber security rules, see our insight Power sector cyber security rules bind vendors from April 2027.

How IndusDesk helps with CERT-In compliance

We watch the authorities, tell you what each change means for your products and plans, represent you while a decision is still open, and carry the work through, with every step on record in your workspace.

Regulatory & trade advisory →

Rule exposure audit →

Talk to our desk about CERT-In compliance Message us on WhatsApp

Frequently asked questions

Is using a VPN legal in India?

CERT-In's directions put their VPN duties on providers, not users: individual citizens aren't covered (CERT-In's FAQ, Q7 and Q34). MeitY's advisory of April 25, 2026 is addressed to VPN providers and other intermediaries. It says giving access to blocked betting and prediction market platforms may breach their due diligence under the IT Rules, 2021 (para 3), which may cost them section 79's protection (para 7).

If you run your own VPN on a rented server, do the CERT-In record rules apply?

The record duty in direction (v) falls on VPN service providers, which CERT-In's FAQ describes as entities offering internet proxy-like services to general internet users (Q34). Individual citizens aren't covered (Q7). The VPS provider you rent the server from is covered by direction (v) and keeps your details as its customer.

Who reports when a vendor is breached, and can a confidentiality clause stop the report?

Any entity that notices the incident must report it to CERT-In, and the duty can't be transferred or contracted away (CERT-In's FAQ, Q13). A confidentiality clause doesn't stop it: the FAQ says the duty overrides any such clause, because section 81 gives the IT Act effect over inconsistent laws (Q22 and Q8). For both reports, CERT-In's and the DPDP Act's, see Data breach reporting in India: CERT-In's 6 hours and DPDP's 72.

Sources

- No. 20(3)/2022-CERT-In, April 28, 2022: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents, directions (i) to (vi), Annexure I and the closing paragraphs
- CERT-In, Frequently Asked Questions on the Cyber Security Directions of 28.04.2022 (May 2022): introduction, para 4 and note; Q2, Q7, Q8, Q13, Q15, Q22, Q23, Q26, Q29, Q30, Q34 to

Q36, Q38, Q40, Q42 and Q43

- No. 20(3)/2022-CERT-In, June 27, 2022: Extension of timelines for the Cyber Security Directions of 28.04.2022 for MSMEs and for validation of subscriber and customer details
- CERT-In web page, Directions by CERT-In under Section 70B, Information Technology Act 2000, as served on October 31, 2026: four items, the directions, the FAQ, the June 2022 extension and "Reporting of a vulnerability"
- MeitY order F. No. P-1501/3/2020-Personnel, October 12, 2026: Declaration of the Indian Computer Emergency Response Team (ICERT) as an Attached Office, paras 1 and 2
- Act No. 10 of 2009: the Information Technology (Amendment) Act, 2008, sections 70B(1), 70B(6) and 70B(7) as inserted
- Act No. 18 of 2023, August 11, 2023: the Jan Vishwas (Amendment of Provisions) Act, 2023, Schedule, serial 32, entry (I)
- S.O. 4745(E), October 31, 2023: the date the Jan Vishwas Act, 2023 amendments to the Information Technology Act, 2000 came into force (November 30, 2023)
- Act No. 22 of 2023, August 11, 2023: the Digital Personal Data Protection Act, 2023, section 2(i)
- G.S.R. 846(E), November 13, 2025: the Digital Personal Data Protection Rules, 2025, rules 1(4), 6(1)(e) and 8(3)
- MeitY advisory No. 2(6)/2024-CL&DG-Part(1), April 25, 2026: to VPN service providers and intermediaries on access to illegal and blocked online betting and prediction market platforms, paras 3 and 7
- CERT-In Security Guidelines CISG-2026-03, version 1.0, June 10, 2026: Guidelines regarding AI-Accelerated Vulnerability Protection and Response Requirements for Original Equipment Manufacturers (OEMs), and Technology Providers, sections 1, 2.1(b), 2.1(c) and 3.1

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

9th Floor, Hemkunt House, Rajendra Place, New Delhi, Delhi 110008, India

Read online: indusdesk.com/meity/cert-in-directions/