PRIXL

PRIXL GUIDE

The Six-Hour Rule

A practical CERT-In incident playbook for small CA firms

Edition 1 · October 2026 · Prixl Technologies

NOT LEGAL ADVICE

This guide summarises the CERT-In Directions of 28 April 2022 for small professional firms and suggests a way to prepare. Confirm how they apply to your firm with a legal advisor, and check CERT-In's website (cert-in.org.in) for the current reporting format and contacts.

Why six hours is less time than it sounds

The CERT-In Directions issued under Section 70B(6) of the IT Act, in force since 27 June 2022 (25 September 2022 for MSMEs), require service providers, intermediaries, data centres, body corporates and government organisations to **report specified cyber incidents to CERT-In within six hours of noticing them**, or of being told about them. CERT-In's own FAQ treats a firm as a body corporate.

Attacks on a server that faces the internet arrive at any hour, nights and weekends included. Incidents rarely start at a convenient time, and the six hours begin when you notice, not when you are ready. A firm that has not prepared will spend most of them finding out whom to call and what to write.

What the directions ask of a firm

Duty	What it means in practice
Report incidents within 6 hours	Send CERT-In a report of a reportable incident within six hours of noticing it. You can send what you know and add details later.
Name a point of contact	One person who deals with CERT-In. Send their name, designation, firm, address, email, mobile and office phone to info@cert-in.org.in, and update it when it changes.
Keep logs for 180 days, in India	Logs of all ICT systems, kept for a rolling 180 days within Indian jurisdiction, to be sent to CERT-In with an incident report or when CERT-In asks. For a Windows server we suggest the full Security, System and Application logs, not only alerts; CERT-In's FAQ asks for failed as well as successful events.
Synchronise clocks	Connect systems to the time servers of NIC or NPL, or to servers traceable to them, so that times in your logs can be trusted.
Answer CERT-In's requests	Provide information or assistance CERT-In asks for, within the time it sets.

The penalty for not complying is set by Section 70B(7) of the IT Act: imprisonment of up to one year, a fine of up to ₹1 crore, or both. The fine limit was raised from ₹1 lakh on 30 November 2023. Reporting is the firm's own duty, which CERT-In's FAQ (Q13) says cannot be transferred, so an IT provider's report does not discharge it.

What counts as an incident

The directions list 20 incident types that must be reported. For a small firm, the ones that matter most are:

- **Unauthorised access** to IT systems or data, such as a stranger signing in to your server.
- **Malicious code**, including ransomware, viruses and trojans.
- **Data breach and data leak**: client data copied or exposed.
- **Attacks on servers** such as database, mail and DNS servers, and on network devices such as routers.
- **Identity theft, spoofing and phishing** attacks.
- **Compromise of critical systems or information.**
- **Unauthorised access to social media accounts**, and attacks on cloud services the firm uses.

Routine background noise is different, though CERT-In's list does include "targeted scanning or probing of critical networks or systems". Password attempts that fail, and connections your firewall drops, happen to every server on the internet all day. Keep the logs of them even when you do not report them. Deciding where noise ends and an incident begins is a judgement. A sign-in that succeeded from an address you do not recognise, an account nobody created, or files that suddenly cannot be opened is not noise. When in doubt, take advice quickly and lean towards reporting.

The first six hours

Hour 0: you notice. An alert, a staff member's call, a ransom note, a client asking about an email you did not send. Write down the time. The clock starts now.

Within the first hour: contain and call.

- Disconnect the affected computer from the network: unplug the cable or turn off Wi-Fi. **Do not switch it off** unless you cannot disconnect it. Shutting down destroys evidence that is still in memory.
- Call the Security Officer, who takes charge, and your IT support.
- Do not delete anything, do not pay or negotiate a ransom before taking expert and legal advice (government agencies advise against paying), and do not try to "clean up".

Hours 1 to 3: establish the facts.

- What happened, and when did it start? Look at alerts and logs. This is where synchronised clocks and kept logs pay off.
- Which systems, accounts and client data are affected?
- Change the passwords of affected accounts from a clean computer.
- Decide with your advisor whether the incident is reportable.

Hours 3 to 6 at the latest: report. Report as soon as you have the basic facts; do not wait for hour six.

- Send the initial report to CERT-In (see the template below) with what you know. Say clearly what is still being investigated.
- Keep a copy, and record the time you sent it.

After the six hours.

- Follow up with CERT-In as facts become clear, and answer its questions.
- Decide with your legal advisor what to tell clients. From May 2027, the DPDP Act also requires telling the Data Protection Board and every affected person of any personal data breach.
- Record the incident in your Security Register, and review it within two weeks: what worked, what did not, and what changes.

From May 2027: the DPDP Act

The Digital Personal Data Protection Rules, notified on 13 November 2025, add a separate duty from May 2027. On any personal data breach, a firm must inform the Data Protection Board and each affected person without delay, and give the Board a detailed account within 72 hours. That runs alongside CERT-In reporting, not instead of it. The same rules require logs to be kept for at least one year. Plan one response that serves both.

Prepare today: a one-page checklist

Item	Done
Security Officer and a deputy named, with mobile numbers written down offline	☐
Point of contact's details sent to info@cert-in.org.in	☐
CERT-In's reporting contacts (email incident@cert-in.org.in, toll-free phone 1800-11-4949, fax 1800-11-6969) and the current reporting form from cert-in.org.in saved offline	☐
IT support, legal advisor and insurer contacts written down offline	☐
Server clocks synchronised to samay1.nic.in, samay2.nic.in or time.nplindia.org (`w32tm /query /status` to check)	☐
Full Windows logs exported daily and kept for 180 days on storage in India (one year from May 2027)	☐
Alerts for failed sign-in bursts, new accounts and a switched-off firewall reach a phone, out of hours too	☐
Backups offline or immutable, and a restore tested this quarter	☐
The report template below filled in as far as possible in advance	☐
A 30-minute rehearsal with the partners: "the server is encrypted at 9 pm on a Saturday"	☐

Initial report template

Prepare this now with everything that does not change, and fill in the rest at the time.

Field	What to write
Organisation	Firm name, address, ICAI firm registration number
Point of contact	Name, role, mobile, email
Time noticed (IST)	Date and time the incident was noticed
Time it started (IST), if known	From alerts and logs
Type of incident	From CERT-In's list, for example unauthorised access or ransomware
Systems affected	Server or computer names, their role, operating system, IP addresses, internet provider, location, and whether it is critical to the firm's work
What happened	A short factual description
Data involved	Kinds of data and whose: clients, staff
Actions taken	Isolated, passwords changed, IT support engaged
Current status	Contained, under investigation, restored
Indicators	Suspicious addresses, file names, emails, if known

PRIXL

About Prixl. Prixl Technologies builds Prixl Warden, which watches the Windows servers of small professional firms and alerts the partners at once when something needs attention, and Prixl Guard for private remote access. A free Information Security Policy template for CA firms is at prixl.io/security-policy. Questions: support@prixl.io.

You may copy, adapt and share this guide under Creative Commons Attribution 4.0 (CC BY 4.0, creativecommons.org/licenses/by/4.0): credit Prixl Technologies, link to the licence and say if you changed it. Not legal advice.