The Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

RFC 2350 v1.0

1. Document Information

This document contains a description of the Indian Computer Emergency Response Team (CERT-In) in accordance with RFC 2350. It provides the basic information about CERT-In, its constituency, functions and responsibilities.

1.1 Date of Last Update

This is the first version of RFC2350 of CERT-In (v1.0 dated 17th March 2022)

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document May Be Found

Available in CERT-In official website at https://www.cert-in.org.in

This version is valid till modified versions are uploaded in the official website of CERT-In.

2. Contact Information

2.1 Name of the Team

Indian Computer Emergency Response Team

Short Name: CERT-In

2.2 Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Communication & information technology
Government of India
Electronic Niketan
6, CGO Complex, Lodhi Road
New Delhi – 110003
India

2.3 Time Zone

Indian Standard Time (GMT+0530)

2.4 Telephone Number

+91-1800-11-4949 (Toll free)
+91-11-24368572 Ext: 111

2.5 Facsimile Number

+91-1800-11-6969 (Toll free)

2.6 Other Telecommunication

+91-11-24368551 Ext: 111

2.7 Electronic Mail Address

Incident Response Help Desk (for cyber security incident report): incident@cert-in.org.in

Information Desk (for security alerts, or any other technical questions/feedback related to cyber security): info@cert-in.org.in, advisory@cert-in.org.in, subscribe@cert-in.org.in

Vulnerability reporting : vdisclose@cert-in.org.in

2.8 Public Keys and Encryption Information

User ID: **incident@cert-in.org.in**
Key ID: 0xB620D0B4
Key Type: RSA
Expires: 2026-12-31
Key Size: 4096/4096
Finger Print: A768 083E 4475 5725 B81A A379 2156 C0C0 B620 D0B4

User ID: **info@cert-in.org.in, advisory@cert-in.org.in, subscribe@cert-in.org.in**
Key ID: 0x275CCACF
Key Type:RSA
Expires: 2026-12-31
Key Size: 4096/4096
Finger Print: EABE 086A 6FC4 CB47 3F29 A90B DE30 A071 275C CACF

User ID: vdisclose@cert-in.org.in
Key ID: 0x3B4E082C
Key Type: RSA

Expires Date: 2026-12-31
Key Size: 4096/4096
Fingerprint: 6927 2217 D8D4 0208 6B1C 23E9 CE29 EA67 3B4E 082C

2.9 Team Members

Director General, CERT-In is the Head of the Organization. CERT-In is an organisation under the Ministry of Electronics and Information Technology (MeitY), Government of India. It has around 100+ officers working at different levels.

2.10 Other Information

CERT-In is a Full Member in FIRST since 2006.

CERT-In is an Operational member of APCERT since 2006.

CERT-In is a listed team in TF-CSIRT since 24th June 2021.

2.11 Points of Customer Contact

Incident Response Help desk (24/7)

Phone: +91-11-24368572, +91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546, +91-1800-11-6969 (Toll Free)

Email: incident@cert-in.org.in

3. Charter

3.1 Introduction

CERT-In is an organisation of Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyber space.

CERT-In provides:

- Proactive services such as Advisories, Security Alerts, Vulnerability Notes, sharing of Indicators of Compromise, Situational awareness of existing & potential cyber security threats and Security Guidelines to help organizations secure their systems and networks

- Reactive services when security incidents occur so as to minimize damage
- Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills.

3.2 Vision

Proactive Contribution in Securing India's cyber space.

3.3 Mission Statement

To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.

3.4 Objectives

- Preventing cyber attacks against the country's cyber space.
- Responding to cyber attacks and minimizing damage and recovery time Reducing national vulnerability to cyber attacks.
- Enhancing security awareness among common citizens.

3.5 Functions/Activities

The Information Technology Act 2000, designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

3.6 Stakeholders

According to the Information Technology Act 2000, CERT-In shall interact and seek assistance from the following stakeholders to collect, share and disseminate information and also to respond and prevent cyber security incidents, namely:-

- Sectoral Computer emergency response teams;
- Intermediaries;
- Internet Registry and Domain registrars;
- Industry;
- Vendors of Information Technology products including security products and services;
- Academia, Research and Development organizations;
- Security and law enforcement agencies;
- Individuals or group of individuals;
- International computer emergency response teams, Forums and expert groups;
- Agency engaged for the protection of critical information infrastructure;
- Department of Telecommunications.

3.7 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Government, Public and Private sectors. In addition, CERT-In provides services to the individuals and home users also.

3.8 Sponsorship and/or Affiliation

CERT-In is functioning under the administrative control of Ministry of Electronics and Information Technology (MeitY), Government of India.

3.9 Authority

CERT-In is designated as the National Nodal Agency for Incident Response under Section 70(B) of the Indian Information Technology Act 2000. The functioning of CERT-In is defined by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

4. Policies

4.1 Types of Incidents and Level of Support

CERT-In provides the following services to its constituency:

- Response to all Cyber security incidents;
- Prediction and prevention of Cyber security incidents;
- Analysis and forensics of cyber security incidents;
- Information security assurance and audits;
- Awareness and technology exposition in the area of cyber security;

- Training or upgrade of technical know-how for its stakeholders.
- Scanning of cyber space with respect to cyber security vulnerabilities, breaches and malicious activities

4.2 Cooperation, Interaction and Disclosure of Information

CERT-In collaborates with:

- Organizations within and outside the country engaged in the specialised areas in protecting and responding to cyber security incidents;
- Organizations engaged in collection of intelligence in general, law enforcement, investigation and forensics;
- Academia, industry, service providers and research and development institutions;
- Individuals or group of individuals.

Disclosure of Information will be followed in accordance to the Indian Constitutional laws.

4.3 Communication and Authentication

CERT-In communicates through e-mail, telephone, postal communication and other possible means of communication based on the Urgency and Sensitivity of the Incident and information.

PGP key signing is used to authenticate the communication made from the Incident Response Helpdesk to its stakeholders.

5. Services

CERT-In operates 24x7 incidence response Help Desk. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services

5.1 Core Services

- Incident Response
    - 24x7 Incident Response Helpdesk
    - Evidence collection & incident investigation
- Prevention and Security Awareness
    - Tracking of Security Threats and Cyber attacks
    - Security Alerts and Advisories
    - Security Workshops and Security Awareness Programs
- Cyber Forensic Lab

- Extract and analyse the data from the digital devices involved in cyber-crimes.

5.2 Security Quality Management Services

- Security Assurance framework and Audit Services
    - Empanelment of Security Auditors for information security audit, including the vulnerability assessment and penetration test
    - episodic security audits of key organizations
- Promotion of Security Best Practices and Security Standards
- Cyber Security Exercises/Drills
- Cyber Crisis Management Plan (CCMP)

5.3 CVE Numbering Authority (CNA)

CERT-In has been undertaking responsible vulnerability disclosure and coordination for vulnerabilities reported to CERT-In since its inception. To move a step further in the direction to strengthen trust in “Make in India” as well as to nurture responsible vulnerability research in the country, CERT-In has now partnered with the CVE Program, MITRE Corporation, USA. In this regard, Indian Computer Emergency Response Team (CERT-In) has been authorized by the CVE Program, as a CVE Numbering Authority (CNA) for vulnerabilities impacting all products designed, developed and manufactured in India.

5.4 Cybersecurity Audit

CERT-In has created a panel of ‘IT security auditing organizations’ for auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the Government, critical infrastructure organizations and those in other sectors of Indian economy.Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Implementation enabling workshops/interactions are conducted periodically. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.

5.5 Cybersecurity Training and Awareness

CERT-In is mandated under Section 70(B) of the Indian Information Technology Act 2000 to conduct cyber security training and awareness programs for its stakeholders in the area of Cybersecurity.

5.6 Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra – https://www.csk.gov.in) has been established by CERT-In for detection of

compromised devices in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The Centre is working in close coordination and in collaboration with Internet Service Providers, antivirus companies, academia and Industry.

6. Incident Reporting

Cybersecurity Incidents can be reported to the 24/7 Incident response Helpdesk at CERT-In through email or Phone.

Phone: +91-11-24368572, +91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546, +91-1800-11-6969 (Toll Free)

Email: incident@cert-in.org.in

An incident reporting form is also available at https://www.cert-in.org.in

7. Disclaimers

CERT-In assumes no responsibility for errors or omissions, or for damages resulting from the use of the information provided in this document.