

# **RFC 2350**

# **CERT La Poste**

Version 1.4 – 2025-02-05

**TLP:CLEAR**

## SUMMARY

1.	Document information .....	4
1.1.	Date of last update.....	4
1.2.	Distribution list for notifications.....	4
1.3.	Locations where this document may be found .....	4
1.4.	Authenticating this document .....	4
1.5.	Document identification .....	4
2.	Contact information.....	5
2.1.	Name of the team.....	5
2.2.	Address.....	5
2.3.	Time zones .....	5
2.4.	Telephone number .....	5
2.5.	Facsimile number .....	5
2.6.	Electronic mail address.....	5
2.7.	Other telecommunication .....	5
2.8.	Public keys and other encryption information .....	5
2.9.	Team members.....	6
2.10.	Other information .....	6
2.11.	Points of customer contact.....	6
3.	Charter .....	6
3.1.	Mission statement.....	6
3.2.	Constituency.....	7
3.3.	Sponsorship and/or affiliation.....	7
3.4.	Authority.....	7
4.	Policies.....	7
4.1.	Types of Incidents and Level of Support .....	7
4.2.	Cooperation, Interaction and Disclosure of Information .....	8
4.3.	Communication and Authentication.....	8
4.4.	Vulnerability responsible disclosure.....	8

5. Services.....	9
5.1. Incident response .....	9
5.2. Proactive activities.....	9
6. Incident Reporting Forms .....	9
7. Disclaimers.....	10

## **1. Document information**

This document contains a description of CERT La Poste in according to RFC 2350, providing basic information about the CERT La Poste team, its channels of communication, its roles and responsibilities.

### **1.1. Date of last update**

This is version 1.4 published the 5th of February 2025

### **1.2. Distribution list for notifications**

Changes to this document are notified by email to:

- InterCERT France / network of French CSIRTs - <https://www.intercert-france.fr/>
- Task Force CSIRT (TF-CSIRT) – <https://www.trusted-introducer.org/>
- FIRST – <https://www.first.org/>

### **1.3. Locations where this document may be found**

The current version of this document is available at CERT La Poste’s website at:

<https://www.lapostegroupe.com/fr/le-cert-du-groupe-la-poste>

### **1.4. Authenticating this document**

This document has been signed with the CERT La Poste’s PGP key. The signature and our public PGP key (ID and fingerprint) are available on our website or on usual large public key-servers (MIT and CIRCL).

### **1.5. Document identification**

Title: “RFC 2350 CERT La Poste”

Version: 1.4

Document date: 05/02/2025

Expiration: this document is valid until superseded by a later version

## **2. Contact information**

### **2.1. Name of the team**

Computer Emergency Response Team – La Poste  
Short name: CERT La Poste

### **2.2. Address**

CERT La Poste  
i-TEAM/STRS/SLCC  
11 Boulevard Général de Gaulle, 44263  
Nantes CEDEX 2  
France

### **2.3. Time zones**

CET – Central Europe Time (UTC/GMT + 1 hour)  
CEST – Central Europe Summertime (UTC/GMT + 2 hours) in Summertime

### **2.4. Telephone number**

Not available

### **2.5. Facsimile number**

Not applicable

### **2.6. Electronic mail address**

To report an information security incident or a cyber threat targeting or involving La Poste Group entities, please contact us at the following address: [cert@laposte.fr](mailto:cert@laposte.fr)

### **2.7. Other telecommunication**

Not applicable.

### **2.8. Public keys and other encryption information**

The CERT La Poste has a PGP key, whose details are:  
User ID: CERT La Poste <cert@laposte.fr>

Key ID: 0xEF8E05FA

Key type: RSA

Key size: 4096

Expires: 07/01/2026

Fingerprint: 0957 735A E0A0 439E 8879 9370 E471 E6D1 EF8E 05FA

The key and its signatures can be found at the usual large public key-servers (MIT and CIRCL).

## **2.9. Team members**

No public information is provided about team members of CERT La Poste.

## **2.10. Other information**

Additional information about CERT La Poste can be found at the following address:

<https://www.lapostegroupe.com/fr/le-cert-du-groupe-la-poste>

## **2.11. Points of customer contact**

The preferred method for contacting CERT La Poste is via e-mail at the address specified in § 2.6.

CERT La Poste can receive incident or vulnerability reports via emails. Please use our cryptographic key to ensure authenticity and confidentiality if needed.

CERT La Poste operates during regular business hours (9:00 AM-6:00 PM GMT+1 from Monday to Friday).

# **3. Charter**

## **3.1. Mission statement**

Le Groupe La Poste (La Poste S.A. and its subsidiaries) is a French group with multiple activities on national and international level, the main ones being:

- Post and parcel delivery services (Colissimo, Chronopost, DPD, Pickup, Stuart, ...)
- Digital services (Digiposte, Identité Numérique, ...)
- Banking and insurance services (La Banque Postale, CNP Assurance)

Entities within Le Groupe La Poste (in French): <https://www.laposte.fr/le-groupe>

Key figures: <https://www.lapostegroupe.com/en/key-figures-of-le-groupe-la-poste>

CERT La Poste is mandated to ensure the cybersecurity of Le Groupe La Poste in cooperation with security operational centres' branches and subsidiaries.

Some of the services provided by CERT La Poste are operated for the benefit of the entire La Poste Group while others are proposed on a voluntary basis and operated in coordination with entities within the scope.

In order to fulfill this mandate CERT La Poste is defined as the main public point of contact for any information technology security issue regarding Le Groupe La Poste and its subsidiaries.

### **3.2. Constituency**

The CERT La Poste constituency covers all users, systems, networks described in § 3.1 including La Poste S.A, its subsidiaries and joint ventures with a majority participation. Its usual geographical zone of intervention is France.

### **3.3. Sponsorship and/or affiliation**

CERT La Poste is a private CERT operated by Le Groupe La Poste. Activities are provided by i-TEAM, an internal division of Le Groupe La Poste S.A.

### **3.4. Authority**

CERT La Poste's mandate covers prevention, detection, and response services as described in Section 5.

## **4. Policies**

### **4.1. Types of Incidents and Level of Support**

CERT La Poste manages all type of incidents which occur or threaten to occur within its constituencies.

The level of support depends on the type and severity of the given security incident, the number of affected entities and CERT La Poste's resource at the time.

CERT La Poste operates on business hours (9am-6pm) but can be reached 24/7/365 using email described in § 2.6.

Any notification should expect a reply within a working day.

## **4.2. Cooperation, Interaction and Disclosure of Information**

CERT La Poste highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams and other organizations which may contribute towards or make use of their services.

CERT La Poste cooperates with French based CSIRT teams listed by:

- InterCERT France: <https://www.intercert-france.fr/>
- ENISA: <https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map>
- Trusted Introducer community: <https://www.trusted-introducer.org/directory/teams.html>
- FIRST: [FIRST Teams](#)

All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted using PGP encryption.

CERT La Poste operates within the boundaries imposed by French and European regulations.

CERT La Poste supports the information sharing Traffic Light Protocol, described on FIRST website:

<https://www.first.org/tlp/>

## **4.3. Communication and Authentication**

PGP based communication should be the standard for sharing any sensitive information, using details mentioned on § 2.8.

As mentioned on § 4.2, CERT La Poste recognizes and follows Traffic Light Protocol labels.

## **4.4. Vulnerability responsible disclosure**

The safety and security of our customers' data, and the reliability of our products and services, are of utmost importance to Le Groupe La Poste.

In case of discovering a security vulnerability, a reporting form is provided to you:

<https://vdp.laposte.fr/p/Security-Information>

## **5. Services**

### **5.1. Incident response**

CERT La Poste handles technical and organizational aspects of information technology security related incidents, including:

- Event analysis
- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

If you need more details on the various incident response' activities specific to a CSIRT, please refer to FIRST resources:

[https://www.first.org/standards/frameworks/csirts/csirt\\_services\\_framework\\_v2.1](https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

### **5.2. Proactive activities**

CERT La Poste offers the following services to its constituency:

- Vulnerability Report intake
- Vulnerability research/discovery
- Vulnerability analysis, coordination, disclosure and response
- Awareness building
- Training and Education
- Exercises
- Technical and Policy Advisory
- Data acquisition
- Analysis and Synthesis
- Communication

If you need more details on the various proactive activities specific to a CSIRT, please refer to FIRST resources:

[https://www.first.org/standards/frameworks/csirts/csirt\\_services\\_framework\\_v2.1](https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

## **6. Incident Reporting Forms**

CERT La Poste does not provide a specific reporting form for reporting incidents. The preferred method for contacting CERT La Poste is via e-mail at the address specified in § 2.6.

Any incident report should contain the appropriate Traffic Light Protocol label detailed in § 4.3, and use PGP encryption with information mentioned in § 2.8 for any sensitive information.

A vulnerability report form is available as specified in § 2.6.

## **7. Disclaimers**

While all precautions are taken in the preparation of information, notifications and alerts, CERT La Poste assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.