DOCAPOSTE

Security Operation Center and Cyber Defense
Description of CSIRT DOCAPOSTE
RFC2350

DOCUMENT MANAGEMENT

Creation Date :	12/02/2018 [DD/MM/AAAA]
Date de la dernière version :	15/09/2025 [DD/MM/AAAA]
Version :	2.0
TLP:	CLEAR

1. DOCUMENT INFORMATION

This document contains a description of CSIRT DOCAPOSTE according to RFC 2350. It provides information about the Computer Security Incident Response Team, how to contact the team, and describes its responsibilities and the services offered by the CSIRT DOCAPOSTE.

1.1 Document revision

This original version was published at: 12-02-2018

1.2 Distribution list for notifications

There is no distribution list for notifications.

1.3 Locations where this document may be found

The current version of this document can be found at:
https://csirt.docaposte.fr/RFC2350_CSIRT_DOCAPOSTE.pdf

1.4 Document authenticity

This document can be retrieved from only this site, using TLS/SSL also signed by the PGP certificate of CSIRT DOCAPOSTE.

2. CONTACT INFORMARTION

This section describes how to contact the CSIRT DOCAPOSTE

2.1 Name of the Team

- CSIRT DOCAPOSTE (C.O.S.C. : Centre Opérationnel de Sécurité et Cyberféfense
- Short name: CSIRT-DOCAPOSTE

2.2 Address

CSIRT DOCAPOSTE / SERES
A l'attention de Serge Carpentier / Julien Rousseau
45 BD Paul Vaillant Couturier
942OO Ivry-Sur-Seine - France

2.3 Time Zone

- CEST / Central European Summer Time

2.4 Telephone Number

- 01 56 29 71 12

2.5 Facsimile Number

- +33 (0) 234 092 746

2.6 Electronic Mail Address

- cert-fr@laposte.fr
- csirt@docaposte.fr

2.7 Public key's and encryption information

Directory PGP DOCAPOSTE

Directory PGP MIT

- Key Id: 0xE93BA775
- Fingerprint: 5209 9E34 2D35 ADAF 3CEF 026C 4E8F 0E31 E93B A775

2.8 Other information

- fast.docaposte.fr
- docaposte.com

2.9 Points of customer contact

The CSIRT of DOCAPOSTE prefers to receive incident reports via e-mail. Please use our cryptographic keys above to ensure integrity and confidentiality.

3. CHARTER

Within this section the CSIRT DOCAPOSTE mandate is discribed

3.1 Mission statement

The CSIRT of DOCAPOSTE’s mission is to coordinate and investigate IT security incident response for the Group DOCAPOSTE. The CSIRT of DOCAPOSTE will investigate any security incident that may involve a DOCAPOSTE Group subsidiaries or DOCAPOSTE as a source or target of an attack or any cyber-threat.

3.2 Constituency

Our constituency are composed of DOCAPOSTE Groupe and all subsidiaries.

3.3 Sponsorship and/or affiliation

The CSIRT of DOCAPOSTE is the Computer Security Incident Response Team (CSIRT) for the Group DOCAPOSTE. His funding is provided by the DOCAPOSTE Group.

3.4 Authority

The CSIRT of DOCAPOSTE coordinate security incidents concerning our constituency.

4. POLICIES

This section describes the policies of DOCAPOSTE CSIRT

4.1 Types of incidents and level of support

The CSIRT of DOCAPOSE addresses all kinds of security incidents which occur, or threaten to occur, within it’s constituency.

4.2 Co-operation, interaction and disclosure of information

The DOCAPOSTE CSIRT's will exchange all necessary information with other CSIRT's as well as with other affected parties if they are involved in the incident response process.

No incident or vulnerability related information will be given to other persons. French law enforcement personnel requesting information in the course of a criminal investigation will be given the requested information within the limits of the court order and the criminal investigation, if they present a valid court order from a French court.

4.3 Communication and authentication

All e-mails sent to the CSIRT of DOCAPOSTE should be signed using PGP. All e-mails containing confidential information should be encrypted and signed using PGP. Information received in encrypted form should not be stored permanently in unencrypted form.

For other communication, a phone call, postal service, or unencrypted e-mail may be used. The CSIRT of DOCAPOSTE supports the Information Sharing Traffic Light Protocol (TLP).

5. SERVICES

This section describes the services the CSIRT DOCAPOSTE offers

5.1 Incident reponse

The team offers the following services:

- Incident analysis
- Incident response support
- Incident response coordination
- Vulnerability response coordination

5.2 Proactive activities

The team offers the following services:

- Intrusion detection services

5.3 Reactive activities

The team offers the following services:

- Awareness building

6. INCIDENT REPORTING FORMS

We do not have an incident reporting form. Please report security incidents via encrypted e-mail to *csirt@docaposte.fr*. DOCAPOSTE CSIRT not have an incident reporting form. Please report security incidents via encrypted e-mail to DOCAPOSTE CSIRT mail contact.

Incident reports should contain the following information:

- Incident date and time (including time zone)
- Source IPs, ports, and protocols
- Destination IPs, ports, and protocols
- Incident type
- And any relevant information

7. DISCLAIMERS

This document is provided ‘as is’ without warranty of any kind, either expressed or implied, but not limited to, this implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

If you notice any mistakes within this document please send a message to us by e-mail. We wille try to resolve such issues as soon as possible.