Security Operation Center and Cyberdefense
Description of CSIRT DOCAPOST
RFC2350

DOCUMENT MANAGEMENT

Creation Date :	12/02/2018 (DD/MM/AAAA)
Date de la dernière version :	12/02/2018 (DD/MM/AAAA)
Version :	1.0
CONFIDENTIALITY	☒C0 ☐C1 ☐C2 ☐C3 ☐C4
TLP	WHITE

1. DOCUMENT INFORMATION

This document contains a description of CSIRT DOCAPOST 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 DOCAPOST.

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.docapost.fr/RFC2350_CSIRT_DOCAPOST.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 DOCAPOST.

2. CONTACT INFORMATION

This section describes how to contact the CSIRT DOCAPOST

2.1 Name of the Team

- CSIRT DOCAPOST (C.O.S.C: Centre Opérationnel de Sécurité et de Cyberdéfense)
- Short name : CSIRT-DOCAPOST

2.2 Address

CSIRT DOCAPOST / SERES
A l'attention de Serge Carpentier / Julien Rousseau
20 Rue Dieumegard
93400 St Ouen – FRANCE

2.3 Time Zone

- CEST / Central European Summer Time

2.4 Telephone Number

- **+ 33 (0) 156 297 711**

2.5 Facsimile Number

- None available

2.6 Other Telecommunication

- None

2.7 Electronic Mail Address

- **csirt@docapost.fr**

2.8 Public key's and encryption information

The CSIRT-DOCAPOST current PGP key may be obtained by sending a request by mail for that at csirt@docapost.fr or is available on:

- PGP DOCAPOST directory: https://pgp.docapost.fr/pks/lookup?op=get&search=0x6F6CB3F6878DA63E
- PGP MIT directory: https://pgp.mit.edu/pks/lookup?op=get&search=0x6F6CB3F6878DA63E

Key ID: 0x878DA63E
Fingerprint: A643 6EF6 58E9 B7F1 3617 415C 6F6C B3F6 878D A63E

2.9 Team members

- The team consists of five people.
- The team consists of IT security analysts.
- No personal information is indicated in this document

2.10 Other information

The DOCAPOST Computer Security Incident Response Team portal is available at : https://csirt.docapost.fr

2.11 Points of customer contact

The CSIRT of DOCAPOST prefers to receive incident reports via e-mail. Please use our cryptographic keys above to ensure integrity and confidentiality. CSIRT DOCAPOST's hours of operation are restricted to regular business hours

- *07:00-20:00 Monday to Friday, all year long.*

3. CHARTER

Within this section the CSIRT DOCAPOST mandate is described.

3.1 Mission statement

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

3.2 Constituency

Our constituency are composed of DOCAPOST Group and all subsidiaries.

3.3 Sponsorship and/or affiliation

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

3.4 Authority

The CSIRT of DOCAPOST coordinate security incidents concerning our constituency.

4. POLICIES

This section describes the policies of DOCAPOST CSIRT

4.1 Types of incidents and level of support

The CSIRT of DOCAPOST addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident.

4.2 Co-operation, interaction and disclosure of information

The DOCAPOST 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 or 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 DOCAPOST 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 DOCAPOST supports the Information Sharing Traffic Light Protocol (TLP).

5. SERVICES

This section describes the services the CSIRT DOCAPOST offers

5.1 Incident response

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 *cisrt@docapost.fr*
DOCAPOST CSIRT not have an incident reporting form. Please report security incidents via encrypted e-mail to DOCAPOST 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, including, but not limited to, the 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 will try to resolve such issues as soon as possible.