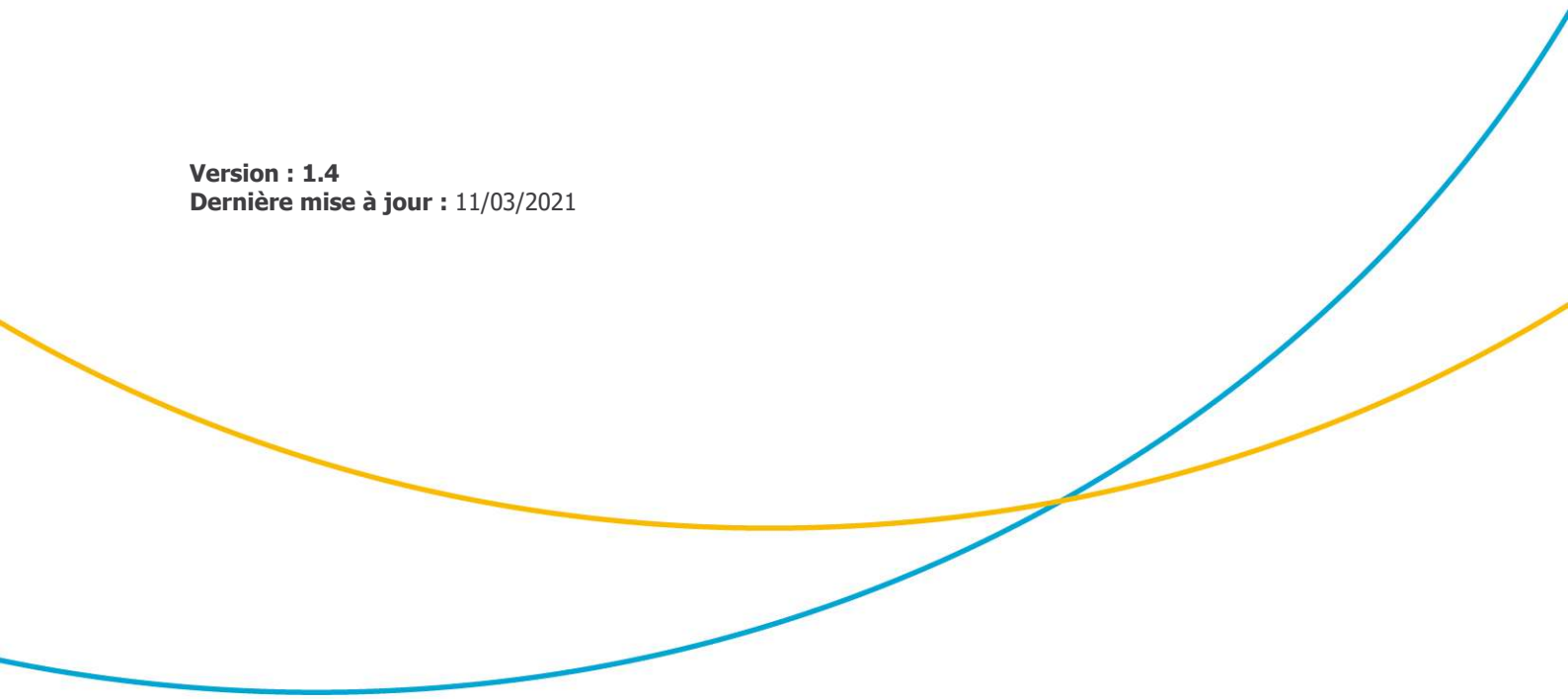
RFC 2350

CSIRT POST CyberForce

Version : 1.4
Dernière mise à jour : 11/03/2021



POST LUXEMBOURG Group

www.postgroup.lu

Document properties

Author	Abdeldjalil BOUROUIS
Name	RFC 2350
Date of creation	11/03/2021
Version	1.4
Classification	C1 – Public / TLP : WHITE
Document owner	CSIRT POST CyberForce

Document status	Approved
Document approved by	**CSIRT POST CyberForce**
Date of approval	11/03/2021

History

Modified by	Date	Version	Description
Abdeldjalil BOUROUIS	11.12.19	0.1	Draft version
Abdeldjalil BOUROUIS	06.01.20	1.0	First version
Abdeldjalil BOUROUIS	16.04.20	1.1	First revision
Abdeldjalil BOUROUIS	09.11.20	1.2	• Update emergency number. • Update Incident report form paragraph.
Abdeldjalil BOUROUIS	26.11.20	1.3	• Update <cybersos(at)post.lu> PGP fingerprint email.
Abdeldjalil BOUROUIS	11.03.21	1.4	• Update web page location to https://www.post.lu/csirt.

Sommaire

1. Document Information 5

1.1 Date of Last Update 5

1.2 Distribution List for Notifications 5

1.3 Locations where this Document May Be Found 5

2 Contact Information 5

2.1 Name of the Team 5

2.2 Address 5

2.3 Time Zone 5

2.4 Telephone Number 5

2.5 Facsimile Number 6

2.6 Other Telecommunication 6

2.7 Electronic Mail Address 6

2.8 Public Keys and Encryption Information 6

2.9 Team Members 6

2.10 Operating hours 6

2.11 Other Information 6

2.12 Points of contact 6

3 Charter 7

3.1 Mission Statement 7

3.1 Constituency 7

3.2 Sponsorship and/or Affiliation 7

3.3 Authority 8

4 Policies 8

4.1 Types of Incidents and Level of Support 8
4.2 Co-operation, Interaction and Disclosure of Information 8
4.3 Communication and Authentication 9
5 Services 9
5.1 Incident response 9
Incident Triage 9
Incident Coordination during a CSIRP 9
Incident Resolution 9
5.2 Proactive services 10
CyberSOS program development 10
Announcements 10
6 Incident Reporting Form 10
7 Disclaimer 10

1. Document Information

1.1 Date of Last Update

This is the version 1.4, first version, fourth revision, published on 11th March 2021.

1.2 Distribution List for Notifications

Distribution lists to notify about the changes in this document:

- Board of Directors (COMEX) of POST Luxembourg;
- Members of CSIRT POST CyberForce;
- Members of CyberForce department;
- Members of Service Desks;
- Members of POST Luxembourg security operations having incident response capabilities;
- Chief Risk Officer of POST Luxembourg;
- Chief Information Security Officer of POST Luxembourg;

1.3 Locations where this Document May Be Found

https://www.post.lu/csirt

Please make sure you are using the latest version.

2 Contact Information

2.1 Name of the Team

The name of the team is CSIRT POST CyberForce.

2.2 Address

CSIRT POST CyberForce
POST Group
20 rue de Reims
L-2417 Luxembourg
Grand-Duchy of Luxembourg

2.3 Time Zone

Central European Time (UTC+01:00) Brussels, Copenhagen, Madrid, Paris

2.4 Telephone Number

+352-2424-7999

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

Security incident reports can be submitted in using CyberSOS <cybersos(at)post.lu>. CSIRT POST CyberForce uses <csirt(at)post.lu> as direct team email contact. This email alias relays mail to the human on duty for the CSIRT POST CyberForce.

2.8 Public Keys and Encryption Information

CSIRT POST CyberForce <csirt(at)post.lu> has PGP Fingerprint:

- 6586 B96E D307 700C 3034 75C6 B6B3 D39C 1C94 BB50

CyberSOS <cybersos(at)post.lu> has PGP Fingerprint:

- F787 796B B0EA 7CF1 AA9F B493 16B0 8428 48A7 4DEF

2.9 Team Members

CSIRT POST CyberForce has security experts, legal and technical support as team members. Abdeldjalil BOUROUIS provide management, liaison and supervision.

2.10 Operating hours

CSIRT POST CyberForce operates Monday to Friday 7:30 AM to 4:30 PM.

Outside operating hours, our 24/7 hotline is reachable with the following number: +352-8002-4000.

2.11 Other Information

None available.

2.12 Points of contact

The preferred method for contacting CSIRT POST CyberForce is via e-mail at <csirt(at)post.lu>. We encourage our constituency (POST Luxembourg employees and customers) to use PGP encryption when sending any sensitive information to CSIRT POST CyberForce.

In case of impossibility to use email as a communication mean (for security concerns or internet access unavailability), CSIRT POST CyberForce is reachable by phone during business hours. Off these hours, our On-duty is taking over the call to transmit it to CSIRT POST CyberForce on-duty members.

3 Charter

3.1 Mission Statement

In regards of computer security incidents or cyberattacks, the CSIRT POST CyberForce mission statement is Protecting POST Luxembourg and its customer in:

- Preparing, Elucidating, Analyzing, Containing and Eradicating (PEACE) Cyberattacks;
- Recovering and reinstating services;
- Learn lessons from incidents;
- Continuously improve and prepare to face new attacks as a loop.

The mission statement can be shorten by the following formula: PEACE Cyberattacks. The mission statement is the ultimate goal for CSIRT POST CyberForce.

In satisfying this mission, CSIRT POST CyberForce contributes to diminish the number of incident and their effects for customers.

3.1 Constituency

CSIRT POST CyberForce is the CERT for POST Luxembourg and POST Telecom S.A.

The constituency covers:

- All the domains owned by POST Luxembourg such as (non-exhaustive):
  - post.lu ;
  - pt.lu ;
  - ept.lu ;
  - postgroup.lu ;
  - posttechnologies.lu ;
  - eservices.lu.
- POST Luxembourg Internet Public ASN AS6661
- All customers that has subscribed to CyberSOS services,

3.2 Sponsorship and/or Affiliation

CSIRT POST CyberForce is the CERT for POST Luxembourg and its customers. CSIRT POST CyberForce is affiliate to POST CyberForce department of POST Telecom S.A and POST Luxembourg integrated entities.

POST Luxembourg integrated entities are:

- POST Group
- POST Telecom S.A.
- POST Finance
- POST Technologies
- POST Courrier

3.3 Authority

CSIRT POST CyberForce operates under the auspices of, and with authority delegated by the executive committee of POST Luxembourg on July 23rd 2020.

4 Policies

4.1 Types of Incidents and Level of Support

CSIRT POST CyberForce addresses all types of computer security incidents, which occur, or threaten to occur, in the constituency networks.

CSIRT POST CyberForce level of support cover:

- High impact and high urgency incident;
- Uncovered incidents by CyberSOS services;
- Vulnerabilities on the behalf of the constituency.

CSIRT POST CyberForce will provide support as much as possible depending of the team workload and the information completeness to handle an incident.

POST Luxembourg Customers can use CyberSOS services for first help and assistance.

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT POST CyberForce exchanges all necessary information as well with other CSIRTs as inside the constituency. CSIRT POST CyberForce do not exchange or disclose personal data without always requiring the explicit consent of the data owner.

CSIRT POST CyberForce cooperate and interact in the context of POST Luxembourg policy called "Politique de gestion des incidents de sécurité CyberSOS" literally translated as "Computer security incident management policy CyberSOS."

CSIRT POST CyberForce, with the support of POST Luxembourg legal department and the central inspection of POST Luxembourg, cooperate with law-enforcement agencies.

All data exchanged, including personal and sensible data, are PGP encrypted in case of transmission in an untrusted and unsecured environment.

4.3 Communication and Authentication

The preferred method to contact CSIRT POST CyberForce is email digitally signed in using a PGP key.

In case sensitive and private data use email as a transfer method, CSIRT POST CyberForce will use encryption.

All e-mail or data communication originating from CSIRT POST CyberForce outside the constituency will use digital signature for each email.

CSIRT POST CyberForce considers telephones using owned by POST Luxembourg networks as trusted and enough secured to not use an encryption layer.

5 Services

CSIRT POST CyberForce helps teams inside the constituency having an incident response capability handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management.

5.1 Incident response

Incident Triage

- Evaluation of the event reported;
- Identification of incidents from events or adverse events;
- Identification of fulfilment to trigger a CSIRP process.

Incident Coordination during a CSIRP

- Determining the root cause of the incident;
- Facilitating contact with other entities, department and services of the constituency;
- Facilitating contact with appropriate law enforcement officials, if necessary;
- Making reports for the entity;
- Communication inside and outside the constituency;
- Ensuring adequate threat sharing information to satisfy regulatory or legal obligations.

Incident Resolution

- Collecting evidence before resolution operation;
- Eradicating the threat from the system affected;
- Assistance by recovering system and/or networks by:;
    - Patching vulnerabilities;
    - Secure the system and/or network to avoid new incidents;
- Assistance for incident aftermath by:
    - Providing a list of actions to avoid new incident occurrence;
    - Lessons learned to enhance existing process and procedure of CSIRP and CyberSOS.

5.2 Proactive services

CyberSOS program development

CSIRT POST CyberForce administrate and manage the governance of security incident management inside the constituency as known as CyberSOS. In this context, CSIRT POST CyberForce provides services by:

- Building new defenses process and procedures;
- Providing CyberSOS Certifications and training;
- Provisioning information in regards of past incident;
- Auditing performance of incident handing with metrics.

Announcements

CSIRT POST CyberForce performs also Announcements in regards of intrusion alerts, vulnerability warnings and security advisory.

6 Incident Reporting Form

CSIRT POST CyberForce provides a form to report security incidents. We strongly encourage anyone reporting an incident to fill it out. CSIRT POST CyberForce report form is available in the following location:

- https://www.post.lu/documents/10181/9693608/Formulaire+CyberSOS+Incident

CSIRT POST CyberForce advises to use email to report security incidents to <cybersos(at)post.lu>, preferably in using PGP.

7 Disclaimer

While CSIRT POST CyberForce will take every precaution in the preparation of information, notifications and alerts, it assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.