RESTENA CSIRT - RFC2350

POL-RFC2350 - Final

Reference: **RFC2350-v4.0**

Version: 4.0

Date: 06.11.24

Classification : Public

TLP: CLEAR

Revision Control

Version	Date	Modification	Status	Origin
1.0	16/03/2008	Initial version	Final	MS
1.1	11/10/2012	Template update, key update, team members	Final	CW
2.0	18/02/2020	New template, update logo, team members, applying new policies	Final	CW
2.1	11/04/2024	changes of members and new keys	Draft	CW
2.2	17/07/2024	Review, Final PGP key updates	Draft	MS
3.0	24/07/2024	Final version	Final	CW
3.1	06/11/2024	review and update of address and members	Draft	CW
4.0	06/11/2024	final version	Final	CW

Contents

1. Introduction

1.1 Overview and purpose

This document provides guidelines for reporting security incidents or reporting relevant security issues to the Restena - Computer Security Incident Response Team (CSIRT). The more, this policy aims to provide general information and describe the Restena-CSIRT activities and services.

This document is based on RFC 2350, a document to express the general Internet community's expectations of CSIRTs.

1.2 Scope

This policy solely covers the activities of the Restena-CSIRT and applies to its full constituency.

This policy is in line with the general Information Security Management System within Restena and complies to policies and procedures in place.

1.3 References

[1] TLP- Information Sharing Traffic Light Protocol v.2.0, https://www.first.org/tlp/

RFC 2350: Expectations for Computer Security Incident Response, https://www.ietf.org/rfc/rfc2350.txt

Trusted Introducer directory: https://www.trusted-introducer.org/directory/teams/restena-csirt.html

1.4 Definitions and Abbreviations

Abbreviation	Definition
CSIRT	Computer Security Incident Response Team
PGP	Pretty Good Privacy
RFC	Request for Comments
TI	Trusted Introducer
TLP	Traffic Light Protocol

Description of the Restena-CSIRT

2. About this document

2.1 Version information

Version 3.0, Date : 24/07/2024

2.2 Location of this document

The current version of this policy can be found for download on the Restena website:

https://restena.lu/en/csirt

2.3 Authentication of this document

The CSIRT signatures and the following document are available on the CSIRT website.

3. Contact information

3.1 Name and address of the team

Restena-CSIRT: Restena's Computer Security Incident Response Team

Fondation Restena / **Restena-CSIRT**

2, place de l'université
L-4365 Esch-sur-Alzette
LUXEMBOURG

3.2 Time zone

Central European Time (GMT+0100), daylight saving time applies.

3.3 Contact email address and Phone number

Phone Number: **+352. 42 44 09 1** (office hours, Monday to Friday except holidays)

Email address: **csirt@restena.lu**

3.4 Team members

Team representatives :

- Marc Stiefer
- Cynthia Wagner

Team members :

- Jo Hoffmann
- Denim Latic
- Bruno Prémont
- David Rosada
- Stefan Winter

The Restena Foundation is headed by Gilles Massen, Director of the Restena Foundation.

3.5 PGP keys

- **CSIRT**

This key is to be used for any confidential communication with Restena-CSIRT: communicating vulnerabilities, incidents, questions, as well as signing advisories and related information. The public key can be found on the website and at the usual public key servers.

PGP Key Id: 0xDADBE3E2C87317E8 <csirt@restena.lu>

Fingerprint: 1DB6 71B7 8071 4050 14E3 F654 DADB E3E2 C873 17E8

- **Jo Hoffmann**

PGP Key Id: 0x3753E11A581FE208FA7F <jo.hoffmann@restena.lu>

Fingerprint: BE56D 770BB E1AC4 0BDE3 3753E 11A58 1FE20 8FA7F

- **Denim Latic**

PGP Key Id: 0xA9D95A53E2A9241F <denim.latic@restena.lu>

Fingerprint: 3152 DBF5 CED7 7BFC BFD8 31BE A9D9 5A53 E2A9 241F

- **Bruno Prémont**

PGP Key Id: 0xC941024143740CD8 <bruno.premont@restena.lu>

Fingerprint: B831 D9DB 84F2 E2A3 A18C 58D5 C941 0241 4374 0CD8

- **David Rosada**

PGP Key Id: 0x5D99C27F0FFD7B1F <david.rosada@restena.lu>

Fingerprint: EB2D 808C 8445 99EC 6CAE 438A 5D99 C27F 0FFD 7B1F

- **Marc Stiefer**

PGP Key Id: 0x351D14F80052F9B4 <marc.stiefer@restena.lu>

Fingerprint: 3F9D BB45 92DE C2E6 A6DA 73CF 351D 14F8 0052 F9B4

- **Cynthia Wagner**

PGP Key Id: 0x67655C0142B101D9 <cynthia.wagner@restena.lu>

Fingerprint: CBEA FB4D 42DE CEFB 10A8 D56A 6765 5C01 42B1 01D9

- **Stefan Winter**

PGP Key Id: 0xC0DE6A358A39DC66 <stefan.winter@restena.lu>

Fingerprint: AD30 91F3 AB24 E05F 4F72 2C03 C0DE 6A35 8A39 DC66

3.6 Points of contacts

The preferred method for contacting the CSIRT is via e-mail at **csirt@restena.lu**.

If it is not possible (or not advisable for security reasons) to use email, the CSIRT-team can be reached by telephone during regular office hours.

Please note that Restena-CSIRT is <u>not</u> offering a 24h/7 service.

The hours of operation are generally restricted to regular business hours (08:00-16:45 Monday to Friday except holidays).

3.7 Other information

General information about the Restena-CSIRT, as well as links to various recommended security resources, can be found at https://restena.lu/en/security.

4. Restena-CSIRT Charter

4.1 Mission statement

The mission and goals are:

- to support and coordinate security incident response within the constituency
- to serve as a trusted point of contact and act as clearing house for security incident-related information
- to improve awareness on Cyber/IT security among the constituents
- Share information and threat intelligence with community
- to keep contact with other CSIRT/CERT teams and cooperate with national and international CERT organisations.

4.2 Constituency

Restena-CSIRT is the sectorial CSIRT for research and Education By this, its constituency is the user community of Education and Research, including:

- University of Luxembourg
- Higher education institutions
- Public and private research centers
- Cultural institutions
- Primary and secondary schools
- Individual users
  Restena's individual users as well as small organisations with no or low technical knowledge will be handled through Restena Helpdesk and Restena NOC, which act as clients of the CSIRT on their own.
- Public services operated by the Restena Foundation (like the .lu registry) are also considered as CSIRT clients.

4.3 Sponsorship and authority

Restena-CSIRT operates under the auspices of Restena Foundation. The Restena-CSIRT is mandated by the Restena Foundation management and is operated and staffed by the Restena employees. The CSIRT directly reports to the Security Manager.

It expects to work cooperatively with the responsible staff of the institutions connected to the Restena network. The authority of Restena-CSIRT is established by the governing general conditions.

4.4 Affiliation

Restena-CSIRT has affiliations with other CERT/CSIRT in Luxembourg (cert.lu) and around Europe being an accredited TI-team.

4.5 Types of incidents and level of support

The Restena-CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, within its constituency.

The level of support given by Restena-CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent and the Restena-CSIRT's resources available (on a best effort basis).

Note that no direct support will be given to end users. They are expected to contact their system- or network administrator, and especially the organization's security contact(s) for assistance.

4.6 Disclosure of information

All Restena-CSIRT members protect the confidentiality of provided information, regardless of its origin and of the medium the data is stored. The more, Restena-CSIRT operates on a need-to-know base. Restena-CSIRT members comply by this with the internal Restena Foundation policies.

4.6.1 Protection of information and anonymization

Restena-CSIRT respects in every case while processing and communicating personal data, the requirements defined by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation.

Restena-CSIRT respects information classification as described in its information classification policy (can be provided on demand). Classified information is treated with the same classification level as the original information provided. If the given classification level does not exist an equivalent classification level is applied, as described in section 4.6.3.

The exchange of information (if required or necessary) is carried out in an anonymized way only. Neither personal information (which could specifically identify an attack target or any individuals), nor extra data shall be exchanged unless explicitly authorised by the owner of the data or appropriately anonymised. Sensitive information is only disclosed if needed for resolving an incident. In very rare cases for resolving an incident, Restena-CSIRT can share specific non-anonymised data with trusted closed groups. These exchanges are done respecting applicable laws and always with full consent of the information owner.

Restena-CSIRT operates according to Luxembourg law and regulations. Therefore, Restena-CSIRT may be forced to disclose information to the authorities, pursuant to a Court Order.

4.6.2 Traffic Light Protocol

The following description are taken from the TLP document provided by First [1]:

TLP:RED : For the eyes and ears of individual recipients only. No further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organization involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and their clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization within their community. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

TLP:GREEN: Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

TLP: CLEAR: Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

All sensitive information shared, in particular e-mails which should use encryption in this case, shall be tagged as [*TLP:COLOUR*] where *COLOUR* is either RED or AMBER.

The classification of information should also be clearly visible on the cover and/or in the footer of all documents sent to or issued by Restena-CSIRT. If contact is by phone or video conference, the TLP classifications is preferred and should be stated prior to the delivery of the information.

Default TLP level

TLP:AMBER is defined as the default information disclosure level.

4.7 Communication and authentication

For normal communication not containing sensitive information, Restena-CSIRT will use conventional methods like unencrypted email.

For secure communication, PGP-encrypted email or telephone will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust or by other methods like call-back, mail-back or even face-to-face meeting.

5. Services

Restena-CSIRT will coordinate security incident prevention, handling and response within its constituency.

5.1 Reactive services

These services are offered in reaction to an occurring security incident involving the constituency, be it detected by Restena-CSIRT staff, constituency's staff or reported to the team by another CSIRT or third party.

5.2 Incident response

- Incident triage

- interpretation of incoming security incident reports, tracking and prioritizing them
- determination of the extent or scope of the security incident

- Incident coordination

- contact the involved organisation(s) to investigate the incident and take the appropriate steps;
- notification of other involved parties on a need-to-know basis, as per the information disclosure policy;
- facilitating contact with appropriate security teams and/or law enforcement officials if necessary;
- making reports to other CSIRTs;
- sending announcements to users (members of constituency), if applicable.

- Incident resolution

- Restena-CSIRT will not provide active security incident resolution service to its constituency but may provide advice and provide best practices.

5.3 Proactive services

5.3.1 Awareness and knowledge building

Proactive services are focused on educational aspects:

- increase security awareness and knowledge among the constituents through articles, best practices, or any other information, to explain security best practices and provide advice on precautions to take,
- organize trainings and seminars to keep the constituency up to date,
- the yearly cyberday.lu conference,
- collect statistics about incidents within the constituency.

6. Incident reporting form

All kind of incident notification format is accepted by the CSIRT. To help the notifier, the following information should be included in the notification, or the template of the incident reporting can be used. An appropriate form has been made available for this purpose.

The electronic version of the incident form can be found on the Restena-security section web site:

https://restena.lu/files/inline-images/CSIRTReportingForm.txt

----

RESTENA CSIRT - Incident reporting form

The following form has been developed to ease gathering incident information. If you believe you have been involved in an incident, please complete - as much as possible - the following form, and send it to: csirt@.restena.lu

If you are unable to send email, please fax it to +352 42 24 73

This information will be treated confidentially, as per our Information Disclosure Policy.

This form is an adaptation of CERT/CC's incident reporting form, version 5.2.

Your contact and organisational information

1. name......................:

2. organisation name.........:

3. are you a RESTENA customer.:

3.a if no:

sector type (such as banking, education, energy or public safety)...........:

4. email address.............:

5. telephone number..........:

6. other (fax, ...)..........:

Affected Machine(s)

(duplicate for each host)

7. hostname and IP...........:

8. timezone..................:

9. purpose or function of the host (please be as specific as possible).............:

Source(s) of the Attack

(duplicate for each host)

10. hostname or IP...........:

11. timezone.................:

12. been in contact?.........:

Description of the incident (duplicate in case of multiple incidents)

13. dates....................:

14. methods of intrusion.....:

15. Tools involved...........:

16. Software versions........:

```
17. Intruder tool output

18. Vulnerabilities exploited

19. Other relevant information

---------------------------------------------------------
```

7. Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, Restena-CSIRT assumes no responsibility for errors, omissions, or for damages resulting from the use of the information contained within.