RFC2350 (Public)

Version 8.0 - 2021-08-25 (Final)

Policy (POL 202)

TLP: **TLP:WHITE**

Department: GOVCERT.LU

Contents

1 Introduction **3**
1.1 Overview . . . 3
1.2 Purpose . . . 3
1.3 Scope . . . 3
1.4 References . . . 3
1.5 Definitions and abbreviations . . . 3

2 Document information **4**
2.1 Date of last update . . . 4
2.2 Distribution list for notifications . . . 4
2.3 Locations where this document may be found . . . 4
2.4 Authenticating this document . . . 4

3 Contact information **4**
3.1 Name of the team . . . 4
3.2 Address . . . 4
3.3 Time zone . . . 4
3.4 Telephone number . . . 5
3.5 Facsimile number . . . 5
3.6 Other telecommunication . . . 5
3.7 E-mail address . . . 5
3.8 Public keys and encryption information . . . 5
3.9 Team members . . . 5
3.10 Other information . . . 5
3.11 Points of customer contact . . . 6

4 Charter **6**
4.1 Mission statement . . . 6
4.2 Constituency . . . 6
4.3 Sponsorship and/or affiliation . . . 7
4.4 Authority . . . 7

5 Policies **7**
5.1 Types of incidents and level of support . . . 7
5.2 Co-operation, interaction and disclosure of information . . . 8
5.3 Communication and authentication . . . 8

6 Services **9**
6.1 Incident response . . . 9
6.1.1 Incident triage . . . 9
6.1.2 Incident coordination . . . 9
6.1.3 Incident resolution . . . 10
6.2 Other activities . . . 10

7 Incident reporting forms **10**

8 Disclaimer **11**

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

1 Introduction

1.1 Overview

This document is composed of several sections describing the work of GOVCERT.LU including its MILCERT.LU mandate. Each section gives guidelines and procedures to the constituents for reporting an incident.

1.2 Purpose

This document contains a description of GOVCERT.LU according to *RFC 2350*. It provides information about the computer security incident response team (CSIRT), how to contact the team, and describes its responsibilities and the services offered by GOVCERT.LU.

1.3 Scope

This policy covers GOVCERT.LU constituency.

1.4 References

1. *FRM702.301 - Incident Reporting Form*
2. *POL204 - Information Disclosure Policy*
3. *PRO301 - Incident Reporting Guidelines for Constituents*
4. *ISTLP - Information Sharing Traffic Light Protocol*. Nov. 2009
5. *RFC 2350: Expectations for Computer Security Incident Response*. URL: https://www.ietf.org/rfc/rfc2350.txt
6. *Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental »*, *URL: http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a424/jo*
7. *RFC2350 National CERT*. URL: https://www.govcert.lu/en/ncert/

1.5 Definitions and abbreviations

Abbreviation	Definition
PGP	Pretty Good Privacy
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team

Table 1: Definitions and abbreviations

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

2 Document information

2.1 Date of last update

This is version 8.0, published on 2021-08-25.

This version is valid until superseded by a later version.

2.2 Distribution list for notifications

Changes to this document are not distributed by a mailing-list, RSS or any other mechanism. Please address any specific questions or remarks to GOVCERT.LU email address (see paragraph 3.7).

2.3 Locations where this document may be found

The current version of this document is always available on GOVCERT.LU website at https://www.govcert.lu.

2.4 Authenticating this document

This document has been signed with the PGP key of GOVCERT.LU.

The signature is available on GOVCERT.LU web site https://www.govcert.lu.

3 Contact information

3.1 Name of the team

CERT Gouvernemental Luxembourg.

Short name: GOVCERT.LU.

3.2 Address

Ministère d'État - CERT Gouvernemental (GOVCERT.LU)
46, rue du Château
L-6961 Senningen
Grand Duchy of Luxembourg

3.3 Time zone

CET / CEST

- GMT+01:00 in winter time (from last Sunday in October to last Sunday in March)
- GMT+02:00 during summer time (from last Sunday in March to last Sunday in October)

3.4 Telephone number

Secretariat: (+352) 247-88966

Hotline: (+352) 247-88960 (Outside of business hours, the principle of best effort is applied.)

3.5 Facsimile number

(+352) 247-88964 (this is *not* a secure fax)

3.6 Other telecommunication

Internet Website: https://www.govcert.lu.

3.7 E-mail address

info@govcert.etat.lu: this email address is used to exchange general information. The reporting of incidents (see below) using this email address should be avoided.

soc@govcert.etat.lu: this email address is used for reporting an incident to the Support and Operation Center team of GOVCERT.LU.

3.8 Public keys and encryption information

E-mail addresses (info@govcert.etat.lu and soc@govcert.etat.lu) used by GOVCERT.LU share the same PGP key, as documented below:

- Key Id: 0x87C0EC7D
    - Key Type: RSA-4096
    - Key Fingerprint: BF0089A9 3ACB25BC 55F26CD9 4F371B37 87C0EC7D

The public key and its signatures can be found on well known large public key servers as well as on GOVCERT.LU public web site (https://www.govcert.lu).

This is used to sign any communication from GOVCERT.LU, it is also used for any confidential communication with GOVCERT.LU (incident reports, alerts).

3.9 Team members

GOVCERT.LU team is operated by dedicated staff of IT security experts from the Government of Luxembourg. The full list of GOVCERT.LU team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

3.10 Other information

General information about GOVCERT.LU, as well as links to various recommended security resources, can be found on GOVCERT.LU public web site (https://www.govcert.lu).

3.11 Points of customer contact

The business hours of operation are 08:00 to 12:00 / 13:00 to 17:00 CET / CEST from Monday to Friday except during Luxembourg's public holidays.

All incident reports should be sent to soc@govcert.etat.lu. This email address is preferred for reporting urgent, sensitive, or critical information concerning security events and incidents.

As a rule this is the preferred contact, the use of phone and fax when reporting incidents should be avoided when possible.

GOVCERT.LU encourages its constituents to use secure email (for instance PGP) when exchanging any sensitive information.

4 Charter

4.1 Mission statement

GOVCERT.LU acts at national and international level to protect its constituents and the Grand-duchy of Luxembourg against cyber threats. Its mandates are defined in *Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental »* and encompass:

- providing a single point of contact for cyber security incidents affecting its constituents covering classified and non-classified infrastructures
- providing a monitoring, detection, alert, and response service
- operating a specialized security intervention team
- maintaining a centralized inventory of incidents
- ensuring 24/7 availability in order to respond to large scale cyber crisis
- representing Luxembourg in international meetings in its field of competence
- acting as a military CERT for the processing of computer emergencies

GOVCERT.LU is also mandated to act as national CERT which is covered separately in *RFC2350 National CERT*.

4.2 Constituency

The Constituency of GOVCERT.LU is made of:

- all ministries, administrations and services of the Luxembourgish government
- military organizations and administrations using military system of the Luxembourgish government (e.g. embassies)
- critical infrastructure operators of the Grand-duchy of Luxembourg
- some major players in sensitive sectors within the Grand-duchy of Luxembourg

For a list and more information, please refer to GOVCERT.LU website https://www.govcert.lu.

4.3 Sponsorship and/or affiliation

GOVCERT.LU is fully sponsored by the Government of Luxembourg.

GOVCERT.LU plays a key role within the national cybersecurity committee. GOVCERT.LU maintains affiliations with CERT / CSIRT community by attending to international and European meetings such as FIRST, TF-CSIRT.

GOVCERT.LU is listed by Trusted-Introducer (TI) since 2011, December 23rd.
GOVCERT.LU is listed by FIRST as a full member since 2016, August 4th.

4.4 Authority

GOVCERT.LU is operated by the State Ministry under the auspices of, and with authority delegated by decision of the Council of Government dated of the 15th of July 2011.

Constituents have to report information security incidents to GOVCERT.LU, and also have to provide contact information with regards to information security incidents.

Constituents have to take GOVCERT.LU's advice in consideration, even though the decision to implement certain measures or not will remain their decision. GOVCERT.LU expects to work cooperatively with system administrators from its Constituency.

Members of GOVCERT.LU community who wish to appeal the actions of GOVCERT.LU should contact the Managing Director of GOVCERT.LU.

All members of GOVCERT.LU team have necessary security clearances. As a consequence, they have wide possibilities of interacting with systems, services and system administrators from the constituency of GOVCERT.LU.

GOVCERT.LU operates within the confines imposed by Luxembourg's legislation.

5 Policies

5.1 Types of incidents and level of support

The level of support given by GOVCERT.LU varies depending on the type and severity of the incident, vulnerability or issue as determined by GOVCERT.LU staff, the type of asset, the part of the constituent affected, and GOVCERT.LU's resources at the time.

Information security incidents at constituents registered at GOVCERT.LU will always have priority over incidents at unregistered constituents.

GOVCERT.LU may act upon request of one of its constituents or may act if one of its constituents is involved in an information security incident.

Information security incidents are prioritised according to their apparent severity and extent. Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. GOVCERT.LU will give full support to the system administrator,

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

network administrator, or department head. Only limited support can be given to end users by GOVCERT.LU.

While GOVCERT.LU understands that there exists great variation in the level of system administrator expertise, and while GOVCERT.LU will endeavour to present information and assistance at a level appropriate to each person, GOVCERT.LU cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases, GOVCERT.LU will provide pointers to the information needed to implement appropriate measures.

5.2 Co-operation, interaction and disclosure of information

While there are legal and ethical restrictions on the flow of information from GOVCERT.LU, it acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, GOVCERT.LU will otherwise share information freely when this will assist in resolving or preventing security incidents.

GOVCERT.LU highly regards the importance of operational cooperation and information-sharing between computer security incident response teams (CSIRTs), and also with other organisations which may contribute towards or make use of their services.

GOVCERT.LU protects sensitive information in accordance with relevant regulations and policies within Luxembourg. In particular, GOVCERT.LU respects the sensitivity markings allocated by originators of information communicated to GOVCERT.LU ("originator control").

GOVCERT.LU appends *ISTLP - Information Sharing Traffic Light Protocol* information when sharing information with teams that support it, and will honour such information if present.

The *POL204 - Information Disclosure Policy* applicable to GOVCERT.LU can be found at https://www.govcert.lu.

5.3 Communication and authentication

The preferred method of communication is via email. If it is not possible (or not advisable for security reasons) to use electronic communication (email / web form), GOVCERT.LU can be reached by telephone during time of operation. Outside of business hours a Hotline phone is available where the principle of best effort is applied.

In view of the types of information that GOVCERT.LU deals with, telephones may be considered sufficiently secure to be used even unencrypted. Unencrypted email is generally not considered sufficiently secure, but will be sufficient for the transmission of unclassified / low-sensitivity data.

Where it is necessary to establish trust, for example before relying on information given to GOVCERT.LU, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within the constituency, and with known peer sites, referrals from known trusted people will suffice to identify communication partners. Otherwise, appropriate methods will be used, such as a reaching out to FIRST members, the use of WHOIS and other Internet registration information, etc., along with telephone call-back or email mail-back to ensure that the party is not an impostor. Incoming email whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP is supported by GOVCERT.LU).

Communication security (encryption and authentication) is achieved by various means: PGP or other agreed

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

means, depending on the sensitivity level and context.

When exchanging highly sensitive data by email or any other electronic means (file transfer), encryption (for instance PGP) will be used. Network file transfers will be considered to be similar to email for these purposes: sensitive data should be encrypted for transmission. All sensitive communication to GOVCERT.LU should be encrypted with the GOVCERT.LU team PGP key.

All email or data communication related to an incident originating from GOVCERT.LU are digitally signed using PGP keys mentioned above, or GOVCERT.LU agents' own signature keys.

Use of encryption / digital signature is encouraged when reporting information to GOVCERT.LU, especially when sending sensitive information.

When submitting a report, (1) provide the operator with notice on the urgency along with the report, (2) your need for feedback, and (3) use where possible the form provided in section 7.

6 Services

GOVCERT.LU is authorised to handle and to address all types of information security incidents, involving both classified and un-classified information, in the constituents' networks or systems and services that fall into GOVCERT.LUs mandate.
GOVCERT.LU supports members of its constituency with a set of reactive and proactive services in the field of information / IT security.

6.1 Incident response

GOVCERT.LU coordinates all activities related to incident response within its constituency. We provide support, help, and advice with respect to the following aspects of incident management:

6.1.1 Incident triage

- Investigating whether an incident occurred indeed.
- Determining the extent of the incident.

6.1.2 Incident coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other entities which may be involved.
- Facilitating contact with the constituency and/or appropriate law enforcement officials.
- Coordinate response to (Distributed) Denial of Service incidents.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

6.1.3 Incident resolution

Note: This set of service includes also incident response on-site.

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.
  To make use of GOVCERT.LU's incident response services, please send email as per section 3.7 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.
- The collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise.

6.2 Other activities

- Anti-Phishing notification & closure
- Compromised systems detection
- Stolen credentials notification
- Targeted malware notification
- General security announcements (non-public)
- Development of security tools
- Malware analysis
- Vulnerability notification
- Security trainings
- Penetration testing

7 Incident reporting forms

Reporting an incident can be done following two manners:

- Anonymous manner: reporting an incident using the online form (https://www.govcert.lu). All incident reported by this means is done in an anonymous manner. Incidents submitted by means of this form are encrypted prior transmission.

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

- General manner: reporting an incident using the *FRM702.301 - Incident Reporting Form*. After having filled out the reporting form, send it within the required timeframe (see Table 2 of the *PRO301 - Incident Reporting Guidelines for Constituents* available on https://www.govcert.lu) by email to the following address: **soc@govcert.etat.lu**.

Whenever possible, please report incident through the *FRM702.301 - Incident Reporting Form* available on https://www.govcert.lu.

Reported information will be treated confidentially, as per GOVCERT.LU *POL204 - Information Disclosure Policy*.

8 Disclaimer

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

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu