THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
High Commission for National Protection

Governmental CERT

Information Disclosure Policy (Public)

Version 6.0 - 2024-11-26 (Final)

Policy (POL 204)

TLP: **TLP:CLEAR**

Contents

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

1 Introduction

1.1 Overview

Processing sensitive information is an important aspect of the daily work of GOVCERT.LU. Sensitive information may be received from an incident reporter or other party participating in the incident handling process. Maintaining trust in GOVCERT.LU's ability to protect sensitive information is crucial for the organisation. The information disclosure rules described in this document aim to help the Computer Security Incident Response Team (CSIRT) to maintain this high level of trust.

1.2 Purpose

This policy defines and describes principles that GOVCERT.LU follows to disclose information. It is intended to complement the *POL203 - Information Classification Policy* and the asset management in order to maintain the confidentiality of managed data.

1.3 Scope

The policy covers all information accessed, modified, generated, received, managed, transmitted or stored by GOVCERT.LU.

1.4 References

1. *FRM727.100 - Accord de Non-Divulgation pour les Employés et Prestataires*
2. *POL203 - Information Classification Policy*
3. *Loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité*, *URL: http://data.legilux.public.lu/eli/etat/leg/loi/2004/06/15/n5/jo*
4. *Euratom - Commission Decision of 29 November 2001 amending its internal Rules of Procedure*. Version 2001/844/EC
5. *NATO Security Committee – Directive on the Security of Information*. Version AC/35-D/2002
6. *NATO Security Policy – Security within the North Atlantic Treaty Organisation*. Version C-M(2002)49
7. *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*. May 2016. URL: http://data.europa.eu/eli/reg/2016/679/2016-05-04
8. *Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance — Version 2.0*. Version 2.0. Aug. 2022. URL: https://www.first.org/tlp/docs/tlp-a4.pdf

1.5 Definitions

1. **Information Exchange**: An '*Information Exchange*' can be either in person, as in a meeting of CSIRTs or of a CSIRT with its constituents, or a meeting of just a few security professionals together; it may also take the form of an exchange of e-mails or a phone conversation.

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

1.6 Abbreviations

Abbreviation	Definition
CSIRT	Computer Security Incident Response Team
EU	European Union
LU	Luxembourg
NATO	North Atlantic Treaty Organization
TLP	Traffic Light Protocol

Table 1: Abbreviations

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

2 Responsibility for data management

All members of GOVCERT.LU have the responsibility to protect the confidentiality of managed data, regardless of its format and of the medium the data is stored on or transmitted over in respect of GOVCERT.LU's internal policies.

GOVCERT.LU is responsible for implementing appropriate procedural, physical, and technical controls for access to, as well as use, transmission, and disposal of GOVCERT.LU data in compliance with this policy.

In order to avoid any leakage of sensitive information, members of GOVCERT.LU shall disclose information only if necessary and in compliance with the following rules.

3 Information disclosure

3.1 Information protection

GOVCERT.LU complies with the need-to-know principle when exchanging information: information which is not public must NOT be freely delivered, and must ONLY be shared with those who need to know.

Information shall be disclosed according to the original level of confidentiality.

GOVCERT.LU respects the information classification allocated by originators of information communicated to GOVCERT.LU as described in internal policies.

The disclosure of sensitive information shall be done ONLY IF NEEDED for resolving an incident. The subsection 3.3 - *Anonymisation* below, states the principles followed by GOVCERT.LU to disclose such information.

GOVCERT.LU frequently interacts with multiple groups including, but not exclusively, other CSIRTs and parties concerned, administrators, vendors, law-enforcement agencies, press, or others. Information disclosure to these groups shall be managed individually and commensurately with the risk involved in information disclosure. GOVCERT.LU reserves the right to request the signing of *FRM727.100 - Accord de Non-Divulgation pour les Employés et Prestataires* before any information exchange.

In order to exchange restricted information with other partners involved in the investigation of a computer security incident, these sites or CSIRTs' bona fide must be verified.

When communicating with other CSIRTs and sites, GOVCERT.LU will ensure that the information which is made available to others:

- will be signed for integrity and non-repudiation assurance whenever deemed necessary
- will be encrypted for confidentiality protection whenever deemed necessary according to this policy

3.2 Private data protection and legal aspects

GOVCERT.LU shall release information to governing authorities or to authorised third parties whenever there is a legal obligation to do so. However, GOVCERT.LU shall delay this action until such a circumstance has been established irrevocably, e.g. by court order.

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

Every case of processing and communicating personal data shall fulfil in form and content 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*.

Rules relating to the disclosure of North Atlantic Treaty Organization (NATO), European Union (EU), and Luxembourg (LU) classified information must be extended to cover all information systems in order to protect the confidentiality, integrity and availability of these systems and the information they process and transmit.

NATO, EU and LU classification policies and decisions are described in:

- NATO : *NATO Security Policy – Security within the North Atlantic Treaty Organisation*
- NATO : *NATO Security Committee – Directive on the Security of Information*
- EU : *Euratom - Commission Decision of 29 November 2001 amending its internal Rules of Procedure*
- LU : *Loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité*

3.3 Anonymisation

Sensitive information shall be anonymised before it is shared with third parties. 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. Moreover, such information may only be disclosed if this is necessary for resolving an incident.

Where anonymising information would not be practical or counterproductive with regard to the handling of the incident, GOVCERT.LU reserves the right to share specific non-anonymised information with trusted closed groups.

These exchanges are done with respect to the applicable laws and with the explicit approval of the owner of the information to be exchanged.

3.4 The information sharing traffic light protocol (ISTLP)

3.4.1 General principles

In order to protect its information, GOVCERT.LU follows an internal information classification policy described in *POL203 - Information Classification Policy*. When exchanging information, a number of rules are applied by the team. These rules are based on a protocol recognised, supported and widely accepted in the CSIRT Community, namely the *Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance — Version 2.0*.

GOVCERT.LU appends Traffic Light Protocol (TLP) information when sharing information only with teams that support it, and will honour such information if present. If TLP is not supported by the external entity, the classification schemes of both entities must be matched in order to guarantee information confidentiality.

The rules comprising the TLP classification are shown in Table 2.

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

Classification level	Rules to be applied
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 organizations 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 its 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 and its clients and prevent further harm. 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.

Table 2: Definition of the TLP Rules

Consequently, all communications higher than TLP:GREEN, particularly e-mails, shall be tagged as [*TLP*:*COLOUR*] where *COLOUR* is either RED or AMBER.

A similar stamp should be clearly visible on the cover and in the footer of all documents sent to or issued by GOVCERT.LU. If contact is by phone or video conference, the TLP classifications are stated prior to the delivery of the information.

3.4.2 Default TLP level

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

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