# Information Disclosure Policy (Public)

## Version 4.0 - 2020-04-17 (Final)

### Policy (POL 204)

**TLP:** TLP:WHITE

**Classification:** PUBLIC

**Department:** GOVCERT.LU

GOVCERT.lu | CERT gouvernemental Luxembourg

# Contents





50, 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 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 *POL205 - Asset Management Policy* 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. *FRM722.204 - Authorization to Disclose Information*
2. *FRM727.100 - Accord de Non-Divulgation pour les Employés et Prestataires*
3. *POL203 - Information Classification Policy*
4. *POL205 - Asset Management Policy*
5. *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
6. *Euratom - Commission Decision of 29 November 2001 amending its internal Rules of Procedure*. Version 2001/844/EC
7. *ISTLP - Information Sharing Traffic Light Protocol*. Nov. 2009
8. *NATO Security Committee – Directive on the Security of Information*. Version AC/35-D/2002
9. *NATO Security Policy – Security within the North Atlantic Treaty Organisation*. Version C-M(2002)49
10. *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*. Apr. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

## 1.5 Definitions and Abbreviations

### 1.5.1 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.


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

### 1.5.2 Abbreviations

| Abbreviation | Definition |
|---|---|
| CERT | Computer Emergency Response Team |
| CNI | Critical National Infrastructure |
| CSIRT | Computer Security Incident Response Team |
| CTIE | Centre des Technologies de l'Information de l'Etat |
| EC | European Community |
| Euratom | European Atomic Energy Community |
| ECSC | European Coal and Steel Community |
| EU | European Union |
| HR | Human Resources |
| ISTLP | Information Sharing Traffic Light Protocol |
| LU | Luxembourg |
| NATO | North Atlantic Treaty Organisation |
| TLP | Traffic Light Protocol |

Table 1: Definitions and Abbreviations


50, 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 on which the data is stored or over which it is transmitted in respect of GOVCERT.LU's internal policies.

GOVCERT.LU is responsible for implementing appropriate procedural, physical, and technical controls for access to, 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, stated 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 CSIRT and sites, GOVCERT.LU will ensure that the information which is made available to others:

- will be signed for non-repudiation assurance
- 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.


50, 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 NATO, EU, and 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 (e.g. via the *FRM722.204 - Authorization to Disclose Information* document)

## 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 *ISTLP - Information Sharing Traffic Light Protocol*.

GOVCERT.LU appends Traffic Light Protocol 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.


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

| TLP Colour | Rules to be Applied |
|---|---|
| **RED** | Non-disclosable information, restricted exclusively to representatives actually participating in the information exchange.<br>Representatives must not disseminate the information outside the exchange. RED information may be discussed during an exchange, if all the representatives participating subscribe to these rules. Guests and others such as visiting speakers who are not full members of the exchange will be required to leave before such information is discussed. |
| **AMBER** | Limited disclosure, restricted to members of the information exchange, people within their organisations and/or constituencies (whether direct employees, consultants, contractors or out-source staff working for the organisation) who need to know in order to take action. |
| **GREEN** | Information may be shared with other organisations, information exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web. |
| **WHITE** | Information that is for public, unrestricted dissemination, publication, web-posting or broadcasting. Any member of the information exchange may publish the information, subject to copyright.<br>Confidential and internal classified information must not be disclosed using the white colour. |

Table 2: Definition of the TLP Rules

Consequently, all communications higher than 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

AMBER is defined as the default information disclosure level.


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