TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

GUIDELINES

TRAFFIC LIGHT PROTOCOL (TLP)

VERSION 2.0

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 11 Jan 2024
Version: 2.5 EN
Author: CyTRIS, CTI department of the CCB

Target audience:
Public

Permitted distribution of TLP:CLEAR
Recipients can spread this to the world, there is no limit on disclosure.

Table of Contents

INTRODUCTION

The Centre for Cybersecurity Belgium (CCB) uses the “Traffic Light Protocol”, or TLP for short. This has been developed to facilitate and encourage the exchange of information in a safe manner.

In August 2022, version 2 was released by the FIRST, the developer of TLP. There are two important changes with the first version:

- TLP:WHITE is replaced by TLP:CLEAR
- TLP:AMBER+STRICT is introduced to indicate that information can only be shared within the organisation of the recipient.

What is TLP?

The protocol requires that the person sending information assigns it a colour using a colour code. This colour indicates if and in what ways this information may be further disseminated. Someone who receives information, and believes that certain information can be disseminated on a greater scale, must ask for permission from the sender first.

Why use TLP?

CCB works in close collaboration with various (international) organisations to identify cyber incidents and to coordinate responses to those incidents. Such activities require trust between all parties involved. Clear information-sharing rules and agreements can ensure this mutual trust. We therefore consider correct application and compliance with TLP of paramount importance.

The TLP provides a simple and intuitive scheme to indicate when and how sensitive information can be disseminated within the worldwide cybersecurity community. The sharing of this information ensures more frequent and effective collaboration between CCB and its partners.

Who uses TLP?

Besides CCB, numerous public services and private businesses across the world use TLP:

- National and organisational Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT)
- International standards and coordination bodies
- Private sector and cybersecurity vendors
- Government intelligence agencies and law enforcement

USAGE

According to FIRST[1], the guidelines for using TLP are as follows:

- **In messaging (e-mail, chat)**:
  TLP-labeled messaging must include the information's TLP label, as well as any additional restrictions, directly before the information itself. The TLP label should appear in the email subject line. Where applicable, indicate the end of the text to which the TLP label applies.

- **In documents**:
  TLP-labeled documents must indicate the TLP label of the information, as well as any additional restrictions, in the header of each page. The TLP label should be in 12-point type or greater for users with low vision. It is recommended to right-justify TLP labels.

The standard by FIRST determines to use colours on a black background. The CCB, however, sometimes opt to deviate from that requirement for practical reasons.

[1] FIRST developed TLP v2. More information can be found here: https://www.first.org/tlp/

TLP LABELS

The four TLP labels are: TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR:

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 organisations 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 organisation and its clients.

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 organisations involved.

Recipients may share TLP:AMBER information with members of their own organisation and its clients, but only on a need-to-know basis to protect their organisation and its clients and prevent further harm.

Note: if the source wants to restrict sharing to the organisation only, they must specify TLP:AMBER+STRICT.

TLP:AMBER+STRICT

Same rules as TLP:AMBER apply (see above), but TLP:AMBER+STRICT restricts sharing to the organisation only.

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 organisations 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/defence 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.

In written form, all TLP labels MUST not contain spaces and SHOULD be in capitals. TLP labels MUST remain in their original form, even when used in other languages: content can be translated, but the labels cannot.

FREQUENTLY ASKED QUESTIONS

When information is shared in TLP:GREEN, what is meant by the term "community"?
When labelling information as TLP:GREEN, the sender should define the community. We define a community as a limited set of entities and/or people. Communities could be a sharing group, an industry sector, the law enforcement community, etc. If this label is not present, the community is assumed to be the cybersecurity/defence community.

How do I share TLP:AMBER information with parent organisations, subsidiaries, or clients?
TLP:AMBER data can be shared with parent organisations, subsidiaries, or clients as described by the protocol. However, before sharing the information with these entities, the label must be changed to TLP:AMBER+STRICT to prevent them from sharing the information further with their related organisations without the originator's permission.

For instance, if a cybersecurity vendor receives TLP:AMBER information, it may share it with some of its key clients. To prevent information from being shared beyond the set restrictions, the cybersecurity vendor labels it with TLP:AMBER-STRICT first. As a result, the vendor's clients are unable to share the information any further.

Remember that if the originator intended to share the information with a larger community, he would have used the TLP:GREEN label.

How do I share information if none of the TLP-labels are appropriate for my needs?
As the originator, you have the ability to add additional sharing rules to the TLP-label. That way, you can restrict sharing with certain organisations, nation states, etc.

What do I do when I really need to share information to a party, but I currently cannot because of the restriction applied?
As the receiver, you can request the originator of the information if they could share the information with the party involved themselves, or alternatively alter the TLP code and/or additional restrictions applied.

EXAMPLES

Sharing a TLP:AMBER+STRICT report

When you receive a TLP:AMBER+STRICT report, you can only share the report within your own organisation on a need-to-know basis.

This means you can share the information with:

- Your manager.
- Your co-worker, as long as he or she is part of the same legal entity.
- Your board.
- …

In general, the following restrictions apply:

- You cannot share the report with your clients or subsidiary organisations.
- You cannot share the report with a befriended CISO of another organisation.
- You cannot discuss the report within a sectorial sharing group, like an ISAC.
- You cannot share the report with the vendor of one your security products.
- …

The distributor of the report can apply additional restrictions.

Sharing a TLP:AMBER report

When you receive a TLP:AMBER report, you can only share the report within your own organisation and your clients or subsidiary organisations on a need-to-know basis.

This means you can share the information with:

- Your manager.
- Your co-worker in the same company or in one of its subsidiaries.
- Your board or the board of a subsidiary.
- …

In general, the following restrictions apply:

- You cannot share the report with a befriended CISO of another organisation.
- You cannot discuss the report within a sectorial sharing group, like an ISAC.
- You cannot share the report with the vendor of one your security products.
- …

The distributor of the report can apply additional restrictions.

Sharing a TLP:GREEN report

When you receive a TLP:GREEN report, you can only share the report within the cybersecurity community.

This means you can share the information with:

- The ISAC or other closed security community your part of.
- With the public during a security conference.

- …

In general, the following restrictions apply:

- You cannot share the slides on a public conference page after a presentation.
- You cannot share the report on any other public website.
- …

TERMINOLOGY

Client	An entity or person using services of a certain organisation or company.
Community	A defined, limited set of entities and/or people. Communities could be a sharing group, an industry sector, the law enforcement community, etc.
Subsidiary	A company controlled by a holding company or any similar relationship.