TRAFFIC LIGHT PROTOCOL (TLP)

FIRST Standards Definitions and Usage Guidance

1. Introduction

a. The Traffic Light Protocol (TLP) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information *source*, towards one or more *recipients*. TLP is a set of four labels used to indicate the sharing boundaries to be applied by the recipients. Only labels listed in this standard are considered valid by FIRST.

b. The four TLP labels are: TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR. In written form, they 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.

c. TLP provides a simple and intuitive schema for indicating with who potentially sensitive information can be shared. TLP is not a formal classification scheme. TLP was not designed to handle licensing terms, nor information handling or encryption rules. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.

d. TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated information exchange systems, such as MISP or IEP.

e. TLP is distinct from the Chatham House Rule, but may be used in conjunction when appropriate. When a meeting is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

f. The source is responsible for ensuring that recipients of TLP-labeled information understand and can follow TLP sharing guidance.

g. The source is at liberty to specify additional sharing restrictions. These must be adhered to by recipients.

h. If a recipient needs to share information more widely than indicated by the TLP label it came with, they must obtain explicit permission from the source.

2. Usage

a. How to use TLP in messaging (such as email and chat)

TLP-labeled messaging MUST indicate the TLP label of the information, as well as any additional restrictions, directly prior to the information itself. The TLP label SHOULD be in the subject line of email. Where needed, also make sure to designate the end of the text to which the TLP label applies.

b. How to use TLP in documents

TLP-labeled documents MUST indicate the TLP label of the information, as well as any additional restrictions, in the header and footer 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.

c. How to use TLP in automated information exchanges

TLP usage in automated information exchanges is not defined: this is left to the designers of such exchanges, but MUST be in accordance with this standard.

d. TLP color-coding in RGB, CMYK and Hex

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Note on color-coding: when there is too little color contrast between text and background, those with low vision struggle to read text or cannot see it at all. TLP is designed to accommodate those with low vision. Sources SHOULD adhere to the TLP color-coding to ensure enough color contrast for such readers.

3. TLP definitions

Community: Under TLP, a *community* is a group who share common goals, practices, and informal trust relationships. A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an *organization* is a group who share a common affiliation by formal membership and are bound by common policies set by the organization. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, clients are those people or entities that receive cybersecurity services from an *organization*. Clients are by default included in TLP:AMBER so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility this definition includes stakeholders and constituents.

a. **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.

b. **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.

c. **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.

d. **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.

Notes:
1. This document uses MUST and SHOULD as defined by RFC-2119.
2. Comments or suggestions on this document can be sent to tlp-sig@first.org.