Traffic Light Protocol (TLP) 2.0

Lucimara Desiderá
CERT.br / NIC.br

Oct 12, 2022

Lucimara Desiderá

Security Analyst

CERT.br / NIC.br

TLP:CLEAR

FIRST Standard: Traffic Light Protocol (TLP)

What is TLP?

- a set of **labels**
- 4 colors to indicate the **sharing boundaries**
- optimized for ease of adoption, **human readability** and **person-to-person sharing**
- the **source is responsible for ensuring that recipients understand** and can follow TLP sharing guidance

Why?

- a simple and intuitive schema
- to **facilitate greater sharing** of potentially sensitive information and more **effective collaboration**

Where to use it?

- documents, e-mails, slides, incident notifications
- information sharing platforms, e.g. MISP
- any other place (ex: conferences and meetings)

https://www.first.org/tlp

TLP:CLEAR

TLP 2.0: Why a new version?

Language improvements

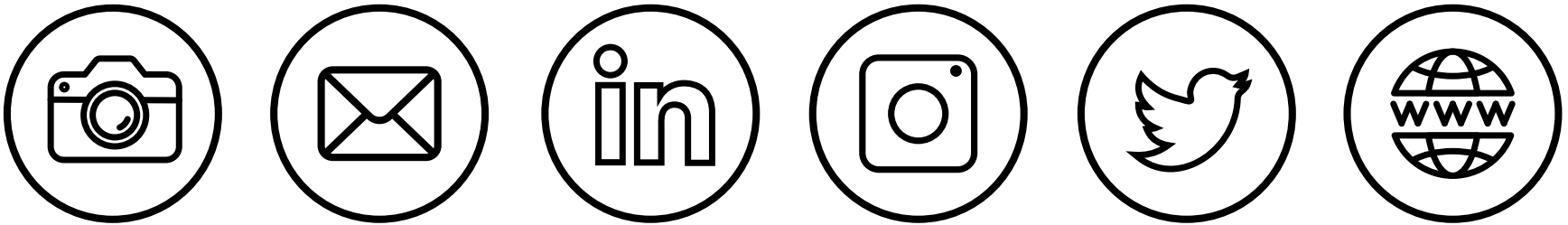
- use the same terms consistently (instead of synonyms)
- less colloquialisms in order to facilitate translations
- clarify the text about sharing boundaries, for example:
  - TLP:RED is for **eyes and ears of individuals** - cannot be used to protect an organization
  - TLP:AMBER and TLP:AMBER+STRICT must be shared on a **need to know basis**

New content

- definition of terms
  - community, organization and clients
- TLP:AMBER+STRICT
- TLP:WHITE ➡ TLP:CLEAR
- color accessibility improvements
- color table with RGB, CMYK and Hexadecimal

TLP:CLEAR

THERE IS NO LIMIT ON DISCLOSURE



https://cert.br/tlp/

TLP:RED

NO FURTHER DISCLOSURE
FOR THE **EYES AND EARS**
OF **INDIVIDUAL RECIPIENTS** ONLY

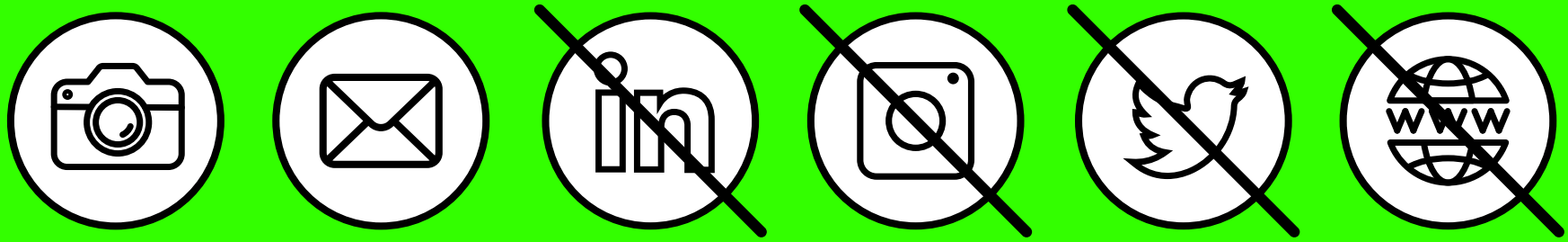
https://cert.br/tlp/

TLP:GREEN

LIMITED DISCLOSURE

CAN SHARE WITHIN YOUR COMMUNITY

BUT NOT VIA PUBLICLY ACCESSIBLE CHANNELS



https://cert.br/tlp/

TLP:AMBER

LIMITED DISCLOSURE, **NEED TO KNOW** BASIS

WITHIN YOUR ORGANIZATION

WITH YOUR CLIENTS

⚠ **IF SHARING** CONSIDER CHANGING TO **TLP:AMBER+STRICT**

https://cert.br/tlp/

TLP:AMBER+STRICT

LIMITED DISCLOSURE, **NEED TO KNOW** BASIS

WITHIN **YOUR ORGANIZATION ONLY**

DO NOT SHARE

WITH CLIENTS OR CONSTITUENCY

https://cert.br/tlp/

TLP	When should it be used?	How can it be shared?
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.**	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.
TLP:AMBER+STRICT **Limited disclosure, recipients can only spread this on a need-to-know basis within their organization only.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. **If the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.**	Recipients **may share TLP:AMBER+STRICT information with members of their own organization only**, but only on a **need-to-know basis** to protect their organization and its clients and prevent further harm.
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**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and	Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Next Steps

- The community needs to **adopt** TLP 2.0 until January 2023!
  - Help to spread the word
  - **Attention**: On **November 1, 2022**, **CISA** will officially adopt TLP Version 2.0
- The SIG will work on documenting “use cases”, for example:
  - What can be shared with service providers and consulting services?
  - In which cases should a TLP:AMBER be changed to TLP:AMBER+STRICT when sharing with clients?
    - How to avoid TLP:AMBER becoming a TLP:GREEN in practice
- Want to help?
  - Join the SIG!
    https://www.first.org/global/sigs/tlp/

References

Standard

- TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0
  https://www.first.org/tlp/
- Press Release: FIRST Releases Traffic Light Protocol Version 2.0 with important updates
  https://www.first.org/newsroom/releases/20220805

TLP 2.0 Launch at FIRST 2022

- Traffic Light Protocol 2022: Updates for An Improved Sharing Experience
  Tom Millar (CISA, US), Don Stikvoort (Elsinore, NL), Ted Norminton (CCCS, CA)
  FIRST Conference 2022, Duration: 1:07:09
  https://youtu.be/2q8IFVOYRjM

CISA

- TRAFFIC LIGHT PROTOCOL (TLP) DEFINITIONS AND USAGE
  https://www.cisa.gov/tlp
  https://www.cisa.gov/sites/default/files/publications/tlp-2-0-user-guide_508c.pdf

Contact

For additional questions, please email:

lucimara@cert.br

TLP:CLEAR