

InfoSec: Traffic Light Protocol

Pavel Růžička <ruza@ruza.eu>




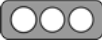


Lightning talks, 08/2017

Current specifications for TLP

- **ISO/IEC 27010:yyyy**, part of the *Standard on Information security management for inter-sector and inter-organizational communications*
- **US-CERT** simple definition
- **Forum of Incident Response and Security Teams (FIRST)**
“..to ensure that interpretations of TLP are consistent, and clear expectations exist across user communities.”

TLP's colours and meanings

-  **RED - personal for named recipients only**
In the context of a meeting. In most circumstances verbally or in person.
-  **AMBER - limited distribution**
The recipient may share information with others within their organization, but only on a 'need-to-know' basis.
-  **GREEN - community wide**
The information may not be published or posted publicly on the Internet, nor released outside of the community.
-  **WHITE - unlimited**
Subject to standard copyright rules, may be distributed freely, without restriction.

Examples

- Mail Subject: “TLP:AMBER New threat on XXX”
- Mail Body: “TLP:AMBER : Organization:BRM-CSIRT”