

Traffic Light Protocol

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

The Traffic Light Protocol (TLP) was created to encourage greater sharing of information. Information sharing is important for helping mitigate the spread of electronic attacks, improving protection through sharing best practices and building trust between players in this field. In order to encourage the sharing of sensitive (but unclassified) information, however, the originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all.

The TLP provides a simple method to achieve this. It is designed to improve the flow of information between individuals, organisations or communities in a controlled and trusted way. It is important that everyone understands and obeys the rules of the protocol. Only then can trust be established and the benefits of information sharing realised. The TLP is based on the concept of the originator labelling information with one of four colours to indicate what further dissemination, if any, can be undertaken by the recipient.

The recipient must consult the originator if wider dissemination is required.

The four colours and their meanings are:

Colour	When should it be used?	How may it be shared?
<p>TLP: RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.</p>
<p>TLP: AMBER</p>  <p>Limited disclosure, restricted to participants' organisations.</p>	<p>Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved.</p>	<p>Recipients may only share TLP: AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP: GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP: GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP: GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community</p>
<p>TLP: WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.</p>

*The NCSC can be contacted by email via info@ncsc.govt.nz or by phone on: **04 498 7654**. We encourage you to contact us at any time if you require any further assistance or advice.*