

交通灯协议（TLP）

FIRST 标准定义和使用指南

1. 介绍

- a. 交通灯协议（TLP）的制定是为了促进潜在敏感信息的更大共享和更有效的协作。信息共享指信息发送方向一个或多个接收方发送信息的过程。TLP 由四个标签组成，用于表明接收方应遵循的共享边界。FIRST 仅承认本标准中定义的标签。
- b. 四个标签分别为：TLP:RED、TLP:AMBER、TLP:GREEN 和 TLP:CLEAR。在书面形式中，在书面形式中，它们不得包含空格并且应该大写。在任何语言中，TLP 标签必须保持其原始形态：内容可以翻译，但标签不能。
- c. TLP 提供了一个简单直观的方案，用于指示潜在的敏感信息的共享范围。TLP 不是正式的分级方案。TLP 的设计目标不是处理许可条款、处理信息或加密规则。TLP 标签及其定义也无意对任何司法管辖区的信息自由或“阳光”法律产生任何影响。
- d. TLP 针对易用性、人类可读性和人与人之间的共享进行了优化；它可以用于自动化信息交换系统，如 [MISP](#) 或 [IEP](#)。
- e. TLP 不同于“查塔姆守则”，但在适当的时候可以结合使用。当根据“查塔姆守则”举行会议时，与会者可以自由地使用所收到的信息，但不得透露信息发送方的身份、任何其他与会者的身份或与会者之间的隶属关系。
- f. 信息发送方负责确保 TLP 标记信息的接收方能够理解并遵循 TLP 共享指南。
- g. 信息发送方可以自由地添加额外的共享限制。信息接收方必须遵守这些规定。
- h. 如果信息接收方需要在 TLP 标签限制的范围外进行信息共享，则必须获得信息发送方的明确许可。

2. 用法

a. 如何在消息中使用 TLP(如电子邮件和聊天)

TLP 标签以及任何附加限制必须在其应用的消息前明确标注。TLP 标签应添加于电子邮件的主题中。必要时，还应在文本末尾添加其适用的 TLP 标签。

b. 如何在文档中使用 TLP

带有 TLP 标签的文档必须在每页的页眉和页脚中注明适用 TLP 标签以及任何附加限制。对于视力欠佳的用户，TLP 标签应使用 12 号或更大的字体。建议将 TLP 标签靠右对齐。

c. 如何在自动化信息共享中使用 TLP

本协议不定义如何在自动化信息共享中使用 TLP：此类定义将由自动交换系统的设计者去决定，但必须符合本标准。

d. TLP 颜色编码（RGB, CMYK 和 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

注：当文本和背景之间的颜色对比度太低时，视力欠佳的人将很难阅读或根本无法区分。TLP 标准的设计考虑了视力欠佳人员的需求。信息发布方应遵守 TLP 颜色编码，以确保其对比度足以满足此类用户需求。

3. TLP 定义

社区：TLP 标准中，社区被定义为具有共同目标、实践和非正式信任关系的群体。一个社区可以类比为 一个国家（或一个部门或地区）的所有网络安全从业者。

组织：TLP 标准中，组织被定义为通过正式成员资格、具有共同隶属关系并遵守组织制定的政策约束的 团体。一个组织可以类比为信息共享组织，但很少有更广泛的。

客户：TLP 标准中，客户被定义为从组织获得网络安全服务的人员或实体。客户被默认包含在 TLP:AMBER 的共享范围中，因此接收方可以向下游进一步共享收到的信息，以便客户采取防卫举措。对于承担国家责任的团队，本定义包括利益相关方及其服务对象。

- TLP:RED** = 不能进一步披露，仅限于接受方的“眼睛”和“耳朵”。当只有披露相关组织的重大隐私、声誉或运营风险才能有效处理该信息时，发布方可以使用 TLP:RED 标签。此时，接收方不得与任何其他共享 TLP:RED 信息。例如，在会议背景中，TLP:RED 信息仅共享于会议的出席人员。
- TLP:AMBER** = 有限的进一步披露，接收方只能在其组织内部及其客户内根据“须知”原则进行传播。注意，**TLP:AMBER+STRICT** 标签将信息的共享限制在组织内部。当信息在相关组织之外共享会带来隐私、声誉或运营风险，而该信息又需要支持才能有效处理时，发布方可以使用 TLP:AMBER 标签。接收方可以与自己组织的成员及其客户共享 TLP:AMBER 信息，但需遵守“须知”

原则，目的是防止组织自身及其用户遭受进一步的破坏。注意：如果发布方想将共享限制在组织自身，则必须使用 TLP:AMBER+STRICT。

- c. **TLP:GREEN** = 有限的进一步披露，接受方可以在其社区中传播收到的信息。当信息有助于提升社区的网安态势时，发布方可以使用 TLP:GREEN 标签。接收方可以与社区内的同行及合作组织共享 TLP:GREEN 信息，但不能通过公开渠道披露该信息。TLP:GREEN 信息不得在社区外共享。注：如果未定义“社区”，则假定为网络安全/防御社区。
- d. **TLP:CLEAR** = 无限制披露，接收方可以将其传播到全世界。当信息仅有很小或没有可预见的滥用风险时，发布方可以使用 TLP:CLEAR 标签并根据有关公开发布规则和程序发布该信息。在版权规则允许范围内，TLP:CLEAR 信息可以不受限制地共享。

注：

- 1. 本文中的必须和应分别对应 [RFC-2119](#) 定义 MUST 和 SHOULD。
- 2. 对此文档的评论或建议可以发送到 tlp-sig@first.org

Translation:	Yuqian Shi, Zhongguancun Laboratory, CN
Review:	Liming Wu, Huawei PSIRT, CN
Review:	Heng Dai, ZTE PSIRT, CN