TRAFFIC LIGHT PROTOCOL (TLP)

FIRST Définitions des Normes et Conseils d'Utilisation

1. Introduction

a. Le protocole TLP (Traffic Light Protocol) a été créé pour faciliter un plus grand partage d'informations potentiellement sensibles et une collaboration plus efficace. Le partage d'informations se fait à partir d'une source d'informations, vers un ou plusieurs destinataires. Le protocole TLP est un ensemble de quatre appellations utilisées pour indiquer les limites de partage à appliquer par les destinataires. Seules les appellations listées dans cette norme sont considérées comme valides par le FIRST.

b. Les quatre appellations du protocole TLP sont : TLP:RED, TLP:AMBER, TLP:GREEN, et TLP:CLEAR. A l'écrit, ils NE DOIVENT pas contenir d'espaces et DOIVENT être en majuscules. Les appellations du protocole TLP DOIVENT rester dans leur forme originale, même lorsqu'ils sont utilisés dans d'autres langues : le contenu peut être traduit, mais pas les labels.

c. Le protocole TLP fournit un schéma simple et intuitif pour indiquer avec qui les informations potentiellement sensibles peuvent être partagées. Le protocole TLP n'est pas un schéma de classification formel. Le protocole TLP n'a pas été conçu pour gérer les termes de licence, ni les règles de traitement de l'information ou de chiffrement. Les appellations du protocole TLP et leurs définitions ne sont pas destinées à avoir un quelconque effet sur la liberté d'accès aux documents administratifs ou les lois dites "sunshine" dans aucune juridiction.

d. Le protocole TLP est optimisé pour la facilité d'adoption, la lisibilité humaine et le partage de personne à personne ; il peut être utilisé dans des systèmes automatisés d'échange d'informations, tels que MISP ou IEP.

e. Le protocole TLP est distinct de la règle de Chatham House, mais peut être utilisé conjointement lorsque cela est approprié. Lorsqu'une réunion se tient selon la règle de Chatham House, les participants sont libres d'utiliser les informations reçues, mais ni l'identité ni l'affiliation du ou des intervenants, ni celle de tout autre participant, ne peuvent être révélées.

f. La source a la responsabilité de s'assurer que les destinataires des informations étiquetées avec le protocole TLP comprennent et sont en mesure de suivre les instructions de partage du protocole TLP.

g. La source est libre de spécifier des restrictions de partage supplémentaires. Celles-ci doivent être respectées par les destinataires.

h. Si un destinataire a besoin de partager l'information plus largement que ce qui est indiqué par le protocole TLP avec lequel elle a été fournie, il doit obtenir la permission explicite de la source.

2. Utilisation

a. Comment utiliser le protocole TLP dans la messagerie (comme le courriel et le chat)

La messagerie étiquetée TLP DOIT indiquer le label TLP de l'information, ainsi que toute restriction supplémentaire, directement avant l'information elle-même. La mention du label TLP DOIT figurer dans la ligne d'objet du courriel. Si nécessaire, veillez également à indiquer la fin du texte auquel s'applique le label TLP.

b. Comment utiliser le protocole TLP dans les documents

Les documents portant un label TLP DOIVENT indiquer le niveau de TLP de l'information, ainsi que toute restriction supplémentaire, dans l'en-tête et le pied de page de chaque page. La mention du protocole TLP DOIT être en caractères de 12 points ou plus pour les utilisateurs malvoyants. Il est recommandé d'ajuster les mentions TLP à droite.

c. Comment utiliser le protocole TLP dans les échanges d'informations automatisés

L'utilisation du protocole TLP dans les échanges d'informations automatisés n'est pas définie : elle est laissée aux concepteurs de ces échanges, mais DOIT être conforme à la présente norme.

d. Codage couleur du TLP en RGB, CMYK et 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

Remarque sur le codage couleur : lorsque le contraste entre le texte et le fond est trop faible, les personnes malvoyantes ont du mal à lire le texte ou ne le voient pas du tout. Le protocole TLP est conçu pour s'adapter aux personnes malvoyantes. Les sources DEVRAIENT adhérer au code couleur du protocole TLP pour assurer un contraste de couleur suffisant pour ces lecteurs.

3. Définitions des appellations utilisées par le protocole TLP

Communauté : Dans le cadre du protocole TLP, une communauté est un groupe qui partage des objectifs, des pratiques et des relations de confiance informelles. Une communauté peut être aussi large que tous les praticiens de la cybersécurité dans un pays (ou dans un secteur ou une région).

Organisation : Dans le cadre du protocole TLP, une organisation est un groupe qui partage une affiliation commune par une adhésion formelle et qui est lié par des politiques communes définies par l'organisation. Une organisation peut être aussi large que tous les membres d'une organisation de partage d'informations, mais rarement plus large.

Clients : Dans le cadre du protocole TLP, les clients sont les personnes ou entités qui reçoivent des services de cybersécurité d'une organisation. Les clients sont inclus par défaut dans l'appellation TLP:AMBER afin que les destinataires puissent partager des informations en aval pour que les clients prennent des mesures pour se protéger. Pour les équipes ayant une responsabilité nationale, cette définition inclut les parties prenantes et les électeurs.

a. **TLP:RED** = Pour les yeux et les oreilles des destinataires individuels uniquement, aucune autre divulgation. Les sources peuvent utiliser l'appellation TLP:RED lorsque les informations ne peuvent pas être traitées efficacement sans risque significatif pour la vie privée, la réputation ou les opérations des organisations concernées. Les destinataires ne peuvent donc pas partager les informations avec l'appellation TLP:RED avec qui que ce soit. Dans le contexte d'une réunion, par exemple, les informations mentionnées avec le label TLP:RED sont limitées aux personnes présentes à la réunion.

b. **TLP:AMBER** = Divulgation limitée, les destinataires ne peuvent diffuser ces informations que sur la base du besoin d'en connaître au sein de leur organisation et de ses clients. Notez que le **TLP:AMBER+STRICT** restreint le partage à l'organisation uniquement. Les sources peuvent utiliser le TLP:AMBER lorsque l'information nécessite un soutien pour être traitée efficacement, mais qu'elle présente un risque pour la confidentialité, la réputation ou les opérations si elle est partagée en dehors des organisations concernées. Les destinataires peuvent partager les informations avec la mention TLP:AMBER avec les membres de leur propre organisation et ses clients, mais uniquement sur la base du besoin d'en connaître, afin de protéger leur organisation et ses clients et d'éviter tout préjudice supplémentaire. Remarque : si la source souhaite restreindre le partage à l'organisation **uniquement**, elle doit spécifier TLP:AMBER+STRICT.

c. **TLP:GREEN** = Divulgation limitée, les destinataires peuvent la diffuser au sein de leur communauté. Les sources peuvent utiliser l'appellation TLP:GREEN lorsque l'information est utile pour accroître la sensibilisation au sein de leur communauté. Les destinataires peuvent partager les informations avec l'appellation TLP:GREEN avec leurs pairs et les organisations partenaires au sein de leur communauté, mais pas via des canaux accessibles au public. Les informations ayant la mention TLP:GREEN ne peuvent pas être partagées en dehors de la communauté. Remarque : lorsque le terme "communauté" n'est pas défini, il s'agit de la communauté de la cybersécurité/défense.

d. **TLP:CLEAR** = Les destinataires peuvent diffuser cette information dans le monde entier, il n'y a pas de limite à la divulgation. Les sources peuvent utiliser l'appellation TLP:CLEAR lorsque les informations présentent un risque minimal ou nul de mauvaise utilisation, conformément aux règles et procédures applicables à la diffusion publique. Sous réserve des règles standard de copyright, les informations mentionnées en TLP:CLEAR peuvent être partagées sans restriction.

Notes:
1. Ce document utilisent les termes DOIT (MUST) et DEVRAIT (SHOULD) tel que défini dans le RFC-2119.
2. Tous les commentaires et ou suggestions peuvent être envoyées à l'adresse courriel suivante tlp-sig@first.org.

Translation: Marc-Frederic GOMEZ, CERT Credit Agricole, FR
Louis Rouxel, CERT-FR, FR
Olivier Caleff, FIRST, FR
Review: Don Stikvoort, FIRST liaison member, NL