TRAFFIC LIGHT PROTOCOL (TLP)

Standardele FIRST - Definiții și Ghid de utilizare

1. Introducere

a. Protocolul Traffic Light Protocol (TLP) a fost creat pentru a facilita partajarea mai amplă a informațiilor potențial sensibile și o colaborare mai eficientă. Partajarea informațiilor are loc de la o *sursă* de informații către unul sau mai mulți *destinatari*. TLP este un set de patru etichete utilizate pentru a indica limitele partajării, limite ce urmează să fie aplicate de către destinatari. Numai etichetele enumerate în acest standard sunt considerate valide de către FIRST.

b. Cele patru etichete TLP sunt: TLP:RED, TLP:AMBER, TLP:GREEN și TLP:CLEAR. În forma scrisă, acestea NU TREBUIE să conțină spații și AR TREBUI să fie scrise cu majuscule. Etichetele TLP TREBUIE să rămână în forma lor originală, chiar și atunci când sunt folosite în alte limbi: conținutul poate fi tradus, dar etichetele nu.

c. TLP oferă o schemă simplă și intuitivă pentru a indica cu cine pot fi partajate informațiile potențial sensibile. TLP nu este o schemă de clasificare formală. TLP nu a fost conceput pentru a gestiona licențierea termenilor, nici regulile de manipulare a informațiilor sau de criptare. Etichetele TLP și definițiile lor nu sunt menite să aibă vreun efect asupra libertății de informare sau a așa-numitelor legi "sunshine" (n.t. – reglementări care impun transparență în mediul guvernamental sau de afaceri), oricare ar fi jurisdicția.

d. TLP este optimizat pentru usurință în adoptare, lizibilitate umană și partajare de la persoană la persoană; poate fi folosit în sistemele automate de schimb de informații, cum ar fi MISP sau IEP.

e. TLP este diferit de Regula Chatham House, dar poate fi folosit împreună cu aceasta atunci când este cazul. Atunci când o întâlnire are loc conform Regulii Chatham House, participanții sunt liberi să folosească informațiile primite, dar nu pot dezvălui nici identitatea, nici apartenența vorbitorului(lor) și nici a oricărui alt participant.

f. Sursa este responsabilă pentru a se asigura că destinatarii informațiilor etichetate TLP înteleg și pot respecta regulile de partajare TLP.

g. Sursa are libertatea de a specifica restricții suplimentare de partajare. Acestea trebuie respectate de către destinatari.

h. Dacă un destinatar trebuie să partajeze informații mai larg decât este indicat de eticheta TLP cu care au venit, acesta trebuie să obțină permisiunea explicită de la sursă.

2. Utilizare

a. Cum se utilizează TLP în mesagerie (cum ar fi e-mail și chat)

Mesajele etichetate TLP TREBUIE să indice eticheta TLP a informațiilor, precum și orice restricții adiționale, imediat înainte de informația în sine. Eticheta TLP AR TREBUI să fie inclusă în câmpul de Subiect al e-mailului. Acolo unde este necesar, asigurați-vă, de asemenea, că indicați sfârșitul textului căruia i se aplică eticheta TLP.

b. Cum se utilizează TLP în documente

Documentele etichetate TLP TREBUIE să indice eticheta TLP a informațiilor, precum și orice restricții adiționale, în antetul și subsolul fiecărei pagini. Eticheta TLP AR TREBUI să fie de dimensiunea 12 puncte sau mai mare pentru utilizatorii cu vedere scăzută. Se recomandă alinierea la dreapta a etichetelor TLP.

c. Cum să utilizați TLP în schimburile automate de informații

Utilizarea TLP în schimburile automate de informații nu este definită: această situație este lăsată în seama proiectanților unor astfel de schimburi, dar TREBUIE să fie în conformitate cu acest standard.

d. Codarea culorilor TLP în RGB, CMYK și 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

TRAFFIC LIGHT PROTOCOL (TLP) – Versiune 2.0 https://www.first.org/tlp

Notă privind codurile de culori: când există prea puțin contrast de culoare între text și fundal, cei cu vedere scăzută întâmpină dificultăți la citirea textului sau nu îl pot vedea deloc. TLP este conceput pentru a se adapta celor cu nivel scăzut de vedere. Sursele AR TREBUI să respecte codul de culoare TLP pentru a asigura suficient contrast de culoare pentru astfel de cititori.

3. Definiții TLP

Comunitate: În conformitate cu TLP, o *comunitate* este un grup care împărtășește obiective comune, practici și relații informale de încredere. De exemplu, o comunitate poate cuprinde toți practicienii în securitate cibernetică dintr-o țară (sau dintr-un sector sau regiune).

Organizație: În conformitate cu TLP, o *organizație* este un grup care împărtășește o afiliere comună prin calitatea formală de membru și sunt conectați de politicile comune stabilite de organizație. O organizație poate să cuprindă toți membrii unei organizații de schimb de informații, rareori mai mare.

Clienți: În conformitate cu TLP, *clienții* sunt acele persoane sau entități care primesc servicii de securitate cibernetică de la o *organizație*. Implicit, clienții sunt incluși în TLP: AMBER, astfel încât destinatarii să poată partaja informații mai în aval pentru ca clienții să ia măsuri pentru a se proteja. Pentru echipele cu responsabilitate la nivel național, această definiție include părțile interesate și constituenții.

a. **TLP:RED** = Doar pentru ochii și urechile destinatarilor individuali, fără a se permite nici un fel de divulgare ulterioară a informației. TLP:RED se poate folosi atunci când informațiile nu pot fi utilizate fără riscuri semnificative privind confidențialitatea, reputația sau operațiunile organizațiilor implicate. Prin urmare, destinatarii nu pot partaja informații TLP:RED cu nimeni altcineva. De exemplu, în contextul unei întâlniri, informațiile TLP:RED se limitează strict la persoanele prezente la întâlnire.

b. **TLP:AMBER** = Divulgare limitată, destinatarii pot transmite informația doar în cadrul organizației lor și/sau al clienților acesteia, pe baza nevoii de a o cunoaște **TLP:AMBER+STRICT** restricționează partajarea numai la organizație. TLP:AMBER se poate folosi atunci când informațiile prezintă riscuri pentru confidențialitate, reputație sau operațiuni dacă sunt partajate în afara organizației implicate. Destinatarii pot partaja informații TLP:AMBER cu membrii propriei organizații și/sau clienții acesteia, dar numai pe baza nevoii de a o cunoaște în vederea prevenirii unor daune suplimentare. Dacă sursa dorește să restricționeze partajarea doar la organizația sa, atunci trebuie să specifice TLP:AMBER+STRICT.

c. **TLP:GREEN** = Divulgare limitată, destinatarii pot transmite informația în cadrul comunității lor. TLP:GREEN se poate folosi atunci când informațiile sunt utile pentru a crește gradul de conștientizare în cadrul comunității extinse. Destinatarii pot partaja informații TLP:GREEN cu colegi și organizații din cadrul comunității lor, dar nu prin canale accesibile publicului. Când "comunitatea" nu este definită, se va presupune comunitatea de securitate cibernetică/apărare.

d. **TLP:CLEAR** = Destinatarii pot transmite informația oricui, nu există limitări privind divulgarea. TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.

O schimbare cheie introdusă în TLP v2.0 este înlocuirea termenului TLP:WHITE cu TLP:CLEAR.

S-a mai introdus și un termen adiacent al TLP:AMBER: TLP:AMBER+STRICT. Sursa: Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0

Sursa: Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0

Note:
1. Acest document folosește TREBUIE și AR TREBUI așa cum este definit de RFC-2119.
2. Comentariile sau sugestiile cu privire la acest document pot fi trimise la tlp-sig@first.org.

Traducere: Valeria Popescu, Directoratul Național de Securitate Cibernetică (DNSC), România

Revizuire: Mihai Rotariu, Directoratul Național de Securitate Cibernetică (DNSC), România
Gabriel Ene, Directoratul Național de Securitate Cibernetică (DNSC), România
Valeriu Vraciu, RoCSIRT
Cristian Mihuți, RevelSi CSIRT