



The Traffic Light Protocol

Bazat pe ghidul FIRST - <https://www.first.org/tlp/>

The Traffic Light Protocol (Protocolul/TLP) presupune un set de clasificări a informațiilor sensibile compusă din patru culori care indică limitele divulgării aplicate destinatarului. TLP oferă o schemă simplă și intuitivă folosită pentru a indica circumstanțele distribuirii informației, facilitând o cooperare frecventă și eficace. Protocolul este distinct de regula Chatham House (prin care părțile pot divulga informațiile primite, dar nu și identitatea sau afilierea sursei, nici a celorlalte părți), dar o poate complementa conform deciziei părților implicate în schimbul de informații.

Sursa informației trebuie să se asigure că destinatarii informației înțeleg protocolul TLP și că îl pot respecta.

Dacă un destinatar necesită un schimb mai amplu sau detaliat de informații decât cel permis inițial prin protocolul TLP, acesta trebuie să obțină permisiunea explicită a sursei.

UTILIZARE

În mesaje email

Corespondența prin email trebuie să indice culoarea specifică protocolului în **Subiectul și Corpul mesajului**, înaintea informației sensibile. Clasificarea TLP trebuie marcată cu majuscule - TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE

În documente

Documentele trebuie să indice nivelul de clasificare TLP în **antetul și subsolul fiecărei pagini**. Pentru a evita confuzia cu schemele de marcare existente este recomandată o indentare în partea dreaptă a paginii. Clasificarea TLP trebuie scrisă cu majuscule și cu o dimensiune de 12 puncte sau mai mare.

RGB:

TLP:RED : R=255, G=0, B=51, background: R=0, G=0, B=0 TLP:AMBER : R=255, G=192, B=0, background: R=0, G=0, B=0 TLP:GREEN : R=51, G=255, B=0, background: R=0, G=0, B=0 TLP:WHITE : R=255, G=255, B=255, background: R=0, G=0, B=0

CMYK:

TLP:RED : C=0, M=100, Y=79, K=0, background: C=0, M=0, Y=0, K=100 TLP:AMBER : C=0, M=25, Y=100, K=0, background: C=0, M=0, Y=0, K=100 TLP:GREEN : C=79, M=0, Y=100, K=0, background: C=0, M=0, Y=0, K=100 TLP:WHITE : C=0, M=0, Y=0, K=0, background: C=0, M=0, Y=0, K=100



NECLASIFICAT

CULOARE	SEMNIFICAȚIE	EXEMPLU
<p>RED (ROȘU)</p>	<p>Indisponibil pentru distribuire către alte entități. Disponibil doar pentru destinatari.</p> <p>Sursele pot utiliza TLP: RED atunci când informația nu poate fi accesată în mod eficient de către terți și ar putea avea impact asupra confidențialității, reputației sau operațiunilor unei părți, dacă este utilizat în mod abuziv.</p> <p>Destinatarii nu pot distribui informații clasificate TLP: RED cu niciun actor din afara schimbului, întâlnirii sau conversației specifice în care a fost inițial dezvăluită această informație.</p> <p>În contextul unei întâlniri, de exemplu, informația TLP: RED este limitată la cei prezenți la întâlnire.</p> <p>În cele mai multe cazuri, TLP: RED ar trebui să fie schimbat verbal sau în persoană.</p>	<p>Informații divulgate în cadrul unei întâlniri sau via mesaj electronic direct</p>
<p>AMBER (PORTOCALIU)</p>	<p>Dezvăluire limitată la organizațiile destinatarilor acestei informații.</p> <p>Sursele pot utiliza TLP: AMBER atunci când informațiile necesită sprijin pentru a fi acționate în mod eficient, dar care prezintă riscuri pentru intimitate, reputație sau operațiuni, dacă sunt împărtășite în afara organizațiilor implicate. Destinatarii pot divulga informații TLP AMBER doar cu membri propriei organizații sau clienții care trebuie să cunoască informațiile, pentru a se proteja sau pentru a preveni alte daune. Sursele sunt libere să precizeze limitele suplimentare ale participării: acestea trebuie respectate.</p>	<p>Divulgarea unor informații de tipul indicatorilor de compromis (IoC) către o structură de tip CERT/CSIRT din cadrul unei organizații. Aceste informații pot fi înaintate către SOC (security operation centres – centre de operare a securității) pentru a acționa într-un anumit sens.</p>

NECLASIFICAT

2 / 3



CERT-RO

**CENTRUL NAȚIONAL DE RĂSPUNS LA
INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO**



NECLASIFICAT

GREEN (VERDE)	<p>Distribuirea informației este limitată la o anumită comunitate.</p> <p>Sursele pot folosi TLP: GREEN atunci când informațiile sunt utile pentru conștientizarea tuturor organizațiilor participante, precum și a colegilor din cadrul comunității sau a unui sector mai larg.</p> <p>Destinatarii pot divulga informația TLP: GREEN cu colegii și organizațiile partenere din cadrul sectorului sau comunității lor, dar nu prin intermediul canalelor accesibile publicului.</p> <p>Informațiile din această categorie pot fi difuzate pe scară largă într-o anumită comunitate.</p> <p>Informațiile TLP: GREEN nu pot fi eliberate în afara comunității.</p>	<p>Divulgarea unei analize de malware către un sector specific al unei anumite industrii.</p>
WHITE (ALB)	<p>Dezvăluirea/divulgarea informației nu este limitată în nici un mod.</p> <p>Sursele pot utiliza TLP: WHITE atunci când informațiile au un risc minim sau unul previzibil de utilizare incorectă, în conformitate cu regulile și procedurile aplicabile pentru eliberarea publică.</p> <p>Sub rezerva normelor standard privind drepturile de autor, informațiile TLP: WHITE pot fi distribuite fără restricții.</p>	<p>Consultanța cu privire la securitatea publică.</p>

NECLASIFICAT

3 / 3



www.cert.ro



office@cert.ro



+4031-6202187



Blvd. Mareșal Averescu 8-10, Sector 1, București, 011455