

Protokol semaforu (TLP)

 first.org/tlp

PROTOKOL SEMAVORŮ (TLP)

PRVNÍ definice standardů a návod k použití — verze 2.0

TLP verze 2.0 je aktuální verze TLP standardizovaná společností FIRST. Je to směrodatné od srpna 2022

1. Úvod

A. Protokol TLP (Traffic Light Protocol) byl vytvořen s cílem usnadnit větší sdílení potenciálně citlivých informací a efektivnější spolupráci. Sdílení informací probíhá z informačního *zdroje* směrem k jednomu nebo více *příjemcům*. TLP je sada čtyř štítků používaných k označení hranic sdílení, které mají být aplikovány příjemci. FIRST považuje za platné pouze štítky uvedené v této normě.

b. Čtyři štítky TLP jsou: TLP:RED, TLP:AMBER, TLP:GREEN a TLP:CLEAR. V psané formě NESMÍ obsahovat mezery a MĚLY by být velkými písmeny. Štítky TLP MUSÍ zůstat ve své původní podobě, i když jsou použity v jiných jazycích: obsah lze přeložit, ale štítky nikoli.

C. TLP poskytuje jednoduché a intuitivní schéma pro označení, s kým lze sdílet potenciálně citlivé informace. TLP není formální klasifikační schéma. TLP nebylo navrženo tak, aby zpracovávalo licenční podmínky ani pravidla pro manipulaci s informacemi nebo šifrování. Štítky TLP a jejich definice nemají mít žádný vliv na svobodu informací nebo zákony o „slunečním svitu“ v jakékoli jurisdikci.

d. TLP je optimalizováno pro snadnou adopci, lidskou čitelnost a sdílení mezi lidmi; může být použito v automatizovaných systémech výměny informací, jako je MISP nebo IEP.

E. TLP se liší od Chatham House Rule, ale může být použito ve spojení, pokud je to vhodné. Když se schůzka koná podle pravidla Chatham House Rule, mohou účastníci volně použít obdržené informace, ale nesmí být odhalena totožnost ani příslušnost mluvčího (řečníků) ani jiného účastníka.

F. Zdroj je odpovědný za zajištění toho, aby příjemci informací označených TLP rozuměli pokynům pro sdílení TLP a mohli je dodržovat.

G. Zdroj si může svobodně určit další omezení sdílení. Ty musí příjemci dodržovat.

h. Pokud příjemce potřebuje sdílet informace v širším měřítku, než je uvedeno na štítku TLP, se kterým přišel, musí získat výslovné povolení od zdroje.

2. Použití

A. Jak používat TLP ve zprávách (jako je e-mail a chat)

Zprávy označené TLP MUSÍ uvádět štítek TLP informací, stejně jako jakákoli další omezení, přímo před samotnými informacemi. Štítek TLP BY MĚL být v předmětu e-mailu. V případě potřeby se také ujistěte, že jste označili konec textu, na který se štítek TLP vztahuje.

b. Jak používat TLP v dokumentech Dokumenty označené TLP MUSÍ v záhlaví a zápatí každé stránky uvádět štítek TLP s informacemi a také jakákoli další omezení. Štítek TLP BY MĚL být **12bodový nebo větší** pro uživatele se slabým zrakem. Doporučuje se správně zarovnat štítky TLP.

C. Jak používat TLP v automatizovaných výměnách informací Využití TLP v automatizovaných výměnách informací není definováno: to je ponecháno na konstruktérech takových výměn, ale MUSÍ být v souladu s touto normou.

d. Barevné kódování TLP v RGB, CMYK a Hex

	RGB: písmo			RGB: pozadí			CMYK: písmo				CMYK: pozadí				Hexadecimální: písmo	Hex: pozadí
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP: ČERVENÁ	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: ZELENÁ	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

Poznámka k barevnému kódování: když je mezi textem a pozadím příliš malý barevný kontrast, slabozrací mají potíže se čtením textu nebo jej nevidí vůbec. TLP je navržen tak, aby vyhovoval osobám se slabým zrakem. Zdroje BY MĚLY dodržovat barevné kódování TLP, aby byl pro takové čtečky zajištěn dostatečný barevný kontrast.

3. Definice TLP

Komunita: Podle TLP je *komunita* skupina, která sdílí společné cíle, postupy a neformální vztahy důvěry. Komunita může být tak široká jako všichni odborníci na kybernetickou bezpečnost v zemi (nebo v sektoru či regionu).

Organizace: Podle TLP je *organizace* skupina, která sdílí společnou příslušnost na základě formálního členství a je vázána společnými zásadami stanovenými organizací. Organizace může být tak široká jako všichni členové organizace sdílející informace, ale jen zřídka širší.

Klienti: Podle TLP jsou klienty osoby nebo subjekty, které od *organizace* přijímají služby kybernetické bezpečnosti. Klienti jsou standardně zahrnuti do TLP:AMBER, takže příjemci mohou sdílet informace dále po proudu, aby mohli klienti podniknout kroky k jejich ochraně. U týmů s vnitrostátní odpovědností tato definice zahrnuje zúčastněné strany a složky.

A. **TLP: ČERVENÁ**= Pouze pro oči a uši *jednotlivých* příjemců, žádné další zveřejnění. Zdroje mohou používat TLP:RED, pokud s informacemi nelze účinně jednat bez významného rizika pro soukromí, pověst nebo operace zúčastněných organizací. Příjemci proto nesmějí sdílet informace TLP:RED s nikým jiným. Například v souvislosti se schůzkou jsou informace TLP:RED omezeny na osoby přítomné na schůzce.

b. **TLP: AMBER**= Omezené zveřejnění, příjemci to mohou šířit pouze na základě potřeby vědět v rámci své *organizace* a jejích *klientů*. Všimněte si, že **TLP: AMBER+STRICT** omezuje sdílení pouze na *organizaci*. Zdroje mohou používat TLP:AMBER, když informace vyžadují podporu, aby bylo možné s nimi efektivně jednat, přesto s sebou nese riziko pro soukromí, pověst nebo operace, pokud jsou sdíleny mimo zúčastněné organizace. Příjemci mohou sdílet informace TLP:AMBER se členy své vlastní organizace a jejími klienty, ale pouze na základě potřeby vědět, aby ochránili svou organizaci a její klienty a zabránili dalším škodám. Poznámka: Pokud chce zdroj omezit sdílení **pouze** na organizaci, musí zadat TLP:AMBER+STRICT.

C. **TLP: ZELENÁ**= Omezené zveřejnění, příjemci to mohou šířit v rámci své komunity. Zdroje mohou používat TLP:GREEN, když jsou informace užitečné pro zvýšení povědomí v jejich širší komunitě. Příjemci mohou sdílet informace TLP:GREEN s kolegy a partnerskými organizacemi v rámci své komunity, ale ne prostřednictvím veřejně přístupných kanálů. Informace TLP:GREEN nesmí být sdíleny mimo komunitu. Poznámka: Pokud „komunita“ není definována, předpokládejte komunitu kybernetické bezpečnosti/obrany.

d. **TLP: CLEAR** = Příjemci to mohou šířit do *světa* , zveřejnění není nijak omezeno. Zdroje mohou používat TLP:CLEAR, pokud informace nesou minimální nebo žádné předvídatelné riziko zneužití, v souladu s platnými pravidly a postupy pro zveřejnění. V souladu se standardními pravidly autorských práv mohou být informace TLP:CLEAR sdíleny bez omezení.

Poznámky:

1. Tento dokument používá MUSÍ a MĚL, jak je definováno v RFC-2119 .
2. Komentáře nebo návrhy k tomuto dokumentu můžete zasílat na adresu tlp-sig@first.org .