Trafikklysprotokollen (TLP)

FIRST standarddefinisjon og veiledning for bruk

1. Introduksjon

a. Trafikklysprotokollen (TLP) ble opprettet for å legge til rette for økt deling av potensielt sensitiv informasjon, og for å gjøre samhandling mer effektivt. Informasjonsdeling skjer fra en informasjonskilde til én eller flere mottakere. TLP er et sett med fire merker som brukes for å indikere delingsbegrensninger som mottaker må forholde seg til. Bare merker beskrevet i denne standarden anses som gyldige av FIRST.

b. De fire TLP-merkene er: TLP:RED, TLP:AMBER, TLP:GREEN, og TLP:CLEAR. I skriftlig form SKAL de ikke inneholde mellomrom, og de BØR stå med store bokstaver. TLP-merkene SKAL beholde sin opprinnelige form, selv når de benyttes på andre språk: innhold kan oversettes; ikke merker.

c. TLP gir en enkel og intuitiv måte å indikere med hvem potensielt sensitiv informasjon kan deles. TLP er ikke en formell klassifiseringsordning. TLP ble ikke laget for å håndtere hverken lisensvilkår eller krypteringsregler. TLP-merker vil ikke ha noen effekt på offentlighetslovgivning i noen jurisdiksjon.

d. TLP er optimalisert for enkel anvendelse, lesbarhet og person-til-person-deling; den kan benyttes i automatiserte informasjonsutvekslingssystemer, for eksempel MISP eller IEP.

e. TLP er ikke det samme som Chatham House-regelen, men de kan brukes sammen der det er hensiktsmessig. Når et møte holdes under Chatham House-regelen står deltakerne fritt til å bruke den mottatte informasjonen, men hverken identiteten eller tilknytningen til foredragsholderen(e) eller andre deltakere kan avsløres.

f. Avsender er ansvarlig for å sikre at mottakere av TLP-merket informasjon forstår og kan følge TLP-delingsveiledningen.

g. Avsender står fritt til å spesifisere ytterligere delingsbegrensninger. Disse må følges av mottakerne.

h. Hvis en mottaker trenger å dele informasjon bredere enn det TLP-merkingen tillater, må de innhente eksplisitt tillatelse fra avsenderen.

2. Bruk

a. Hvordan bruke TLP i meldingstjenester (eksempelvis e-post og chat)

TLP-merket melding SKAL angi TLP-merket til informasjonen, samt eventuelle tilleggsbegrensninger, rett før selve informasjonen. TLP-merket BØR stå i emnefeltet i e-post. Der det er nødvendig, sørg også for å angi slutten av teksten som TLP-merkingen gjelder for.

b. Hvordan bruke TLP i dokumenter

TLP-merkede dokumenter SKAL angi gjeldende TLP-merke for informasjonen samt eventuelle tilleggsbegrensninger, i topp- og bunntekst på hver side. TLP-merkingen BØR være i 12 punkts skriftstørrelse eller større for svaksynte. Det anbefales å høyrejustere TLP-merker.

c. Hvordan bruke TLP i automatisk informasjonsutveksling

Bruk av TLP i automatisert informasjonsutveksling er ikke definert: dette er overlatt til utviklerne av slike utvekslinger, men SKAL være i samsvar med denne standarden.

d. TLP fargekoding i RGB, CMYK og 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

Spesielt om fargekoding: Hvis det er for lite kontrast mellom tekst og bakgrunn vil de med dårlig syn ha problemer med å lese teksten eller å se den i det hele tatt. TLP er laget for å legge til rette for dette. Kilder BØR følge fargekodingen for å sørge for riktig kontrast for slike lesere.

3. TLP definisjoner

Miljø: Under TLP er et *miljø* en gruppe som deler felles mål, praksis og uformelle tillitsforhold. Et miljø kan være så omfattende som alle cybersikkerhetsutøvere i et land (eller i en sektor eller region).

Organisasjon: Under TLP er en *organisasjon* en gruppe som deler en felles tilknytning ved formelt medlemskap og er bundet av felles retningslinjer satt av organisasjonen. En organisasjon kan være så omfattende som alle medlemmer av en informasjonsdelingsorganisasjon, men sjeldent større.

Klienter: Under TLP er *klienter* de personene eller entiteter som mottar cybersikkerhetstjenester fra en organisasjon. Klienter er som standard inkludert i TLP:AMBER, slik at mottakerne kan dele

informasjon nedstrøms, slik at klienter skal kunne iverksette tiltak for å beskytte seg selv. For entiteter med nasjonalt ansvar inkluderer denne definisjonen interessenter og målgruppe.

a. **TLP:RED** = Kun for *individuelle, personlige* mottakere. Ingen ytterligere formidling. Avsender kan bruke TLP:RED når informasjon ikke effektivt kan ageres på uten betydelig risiko for personvern, omdømme eller driften til de involverte organisasjonene. Mottakere kan derfor ikke dele TLP:RED-informasjon med noen andre. For eksempel i forbindelse med et møte er TLP:RED-informasjon begrenset til de som er til stede på møtet.

b. **TLP:AMBER** = Begrenset formidling. Mottakere kan bare dele dette videre ved tjenstlig behov i sin egen organisasjon og dens klienter. Merk at **TLP:AMBER+STRICT** begrenser deling til kun organisasjonen. Avsender kan bruke TLP:AMBER når informasjon krever støtte for å effektivt kunne ageres på, men fortsatt medfører risiko for personvern, omdømme eller drift dersom den deles utenfor de involverte organisasjonene. Mottakere kan dele TLP:AMBER-informasjon med medlemmer av sin egen organisasjon og dens klienter, men bare ved tjenstlig behov for å beskytte sin organisasjon og dens klienter og forhindre ytterligere skade. Merk: hvis avsender ønsker å begrense deling til **kun** organisasjonen, må de spesifisere TLP:AMBER+STRICT.

c. **TLP:GREEN** = Begrenset formidling. Mottakere kan spre dette innad i sitt miljø. Avsender kan bruke TLP:GREEN når informasjon er nyttig for å øke bevisstheten i deres bredere miljø. Mottakere kan dele TLP:GREEN-informasjon med kollegaer og organisasjoner i deres sektor eller miljø, men ikke via offentlig tilgjengelige kanaler. TLP:GREEN-informasjon kan ikke deles utenfor miljøet. Merk: når aktuelt miljø ikke er definert, anta cybersikkerhets- eller cyberforsvarermiljøet.

d. **TLP:CLEAR** = Mottakere kan spre dette til *verden*. Det er ingen begrensning på offentliggjøring. Avsender kan bruke TLP:CLEAR når informasjon medfører minimal eller ingen forutsigbar risiko for misbruk, i samsvar med gjeldende regler og prosedyrer for offentlig utgivelse. Med forbehold om opphavsregler kan TLP:CLEAR-informasjon deles uten begrensninger.

Noter:
1. Dette dokumentet bruker SKAL (MUST) og BØR (SHOULD) slik de er definert i RFC-2119.
2. Kommentarer eller forslag til dette dokumentet kan sendes tlp-sig@first.org.

Translation: KraftCERT, NO
Review: UiO-CERT, NO
NCSC, NO