

יום שלישי 12 מרץ 2024
סימובין:

סיווג מידע על פי שיטת הרמזור (TLP¹) גרסה 2.0

שיטת הרמזור הינה שיטה מקובלת לסיווג מידע רגיש שאינו מסווג מבחינה ביטחונית. מטרתה להקל על שיתוף מידע תוך הגדרת מגבלות והתניות לגבי הפצתו. סימון זה יוצר מוסכמה בין השותפים לבין אופן השימוש הנאות במידע, על מנת לאפשר העברת מידע הגנתי חשוב לכל הגורמים הרלוונטיים תוך מזעור החשש לפגיעה בגורם המשתף.

באוגוסט 2022 ארגון FIRST פרסם גרסה חדשה של פרוטוקול TLP: 2.0. בגרסה החדשה קיימים שני שינויים עיקריים:

- **TLP: CLEAR** מחליף את **TLP: WHITE**
- הוספת **TLP: AMBER + STRICT**

אופן שימוש:

1. **כיצד להשתמש בפרוטוקול TLP בעת העברת הודעות (כגון דוא"ל וצ'אט)?**
יש לציין את סיווג ה-TLP של המידע ישירות ולפני המידע עצמו. הסיווג צריך להופיע בשורת הנושא של ההודעה. במידת הצורך יש לציין את המיקום בטקסט בו נגמר סיווג ה-TLP.
2. **כיצד להשתמש בפרוטוקול TLP במסמכים?**
יש לציין את סיווג ה-TLP בכותרת העליונה והתחתונה בצד ימין של כל עמוד. גודל הגופן בו הסיווג צריך להיות כתוב הוא 12 או יותר, עבור משתמשים עם ראייה לקויה.
3. **כיצד להשתמש בפרוטוקול TLP בחילופי מידע אוטומטיים?**
השימוש במצב זה אינו מוגדר. אך קיימת חובה לפעול לפי הסטנדרט.
4. **קידוד צבע TLP ב- RGB, CMYK ו Hex:**
כאשר יש ניגודיות צבע קטנה מדי בין הטקסט לרקע, אנשים בעלי לקויות ראייה מתקשים לקרוא את הטקסט או שלא יכולים לראותו כלל. גווי ה-TLP נועדו להתאים לאנשים בעלי ראייה לקויה. בעת סיווג המסמך לפי הפרוטוקול יש לדבוק בקידוד הצבעים במטרה להבטיח ניגודיות צבע מספקת עבור קוראים אלו.

	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

¹ TLP - Traffic Light Protocol

הגדרות:

- **קהילה:** קבוצה בעלת יחסי אמון לא פורמליים, מטרות ושיטות עבודה משותפות (לדוגמה: כל מנהלי אבטחת המידע במדינה/מגזר/אזור).
- **ארגון:** קבוצה שחולקת שיוך משותף על-ידי חברות רשמית ומחויבת לעמוד בדרישות מדיניות משותפת שנקבעה ע"י הארגון.
- **לקוחות:** אנשים או גופים שמקבלים שירותי הגנת סייבר מהארגון. המטרה היא שהלקוחות יוכלו לנקוט בפעולות על-מנת להגן על עצמם.

סיווג	ייעוד הסיווג	מגבלות השיתוף של הגורם המקבל
TLP: RED	מקרים בהם לא ניתן לפעול ביעילות עם המידע ללא סיכון משמעותי לפרטיות, למוניטין או לפעולות של הארגונים המעורבים	ניתן לשתף מידע המסווג "RED" רק עם קבוצת הנמענים המקורית. מקובל לבצע שיתוף בעל-פה או באופן אישי
TLP: AMBER + STRICT	מקרים בהם שימוש אפקטיבי במידע מצריך שיתוף גורמים נוספים, אך הרחבת התפוצה מעבר לכך עלולה לפגוע בפרטיות, במוניטין או בפעילות הגורם המשתף	ניתן לשתף מידע המסווג "AMBER + STRICT" עם חברי הארגון הנמען בלבד
TLP: AMBER	מקרים בהם שימוש אפקטיבי במידע מצריך שיתוף גורמים נוספים, אך הרחבת התפוצה מעבר לכך עלולה לפגוע בפרטיות, במוניטין או בפעילות הגורם המשתף	ניתן לשתף מידע המסווג "AMBER" עם חברי הארגון הנמען ולקוחותיו
TLP: GREEN	מקרים בהם המידע עשוי להועיל לגורמים רבים ושיתופו אינו כרוך בסיכון לגורם המשתף	ניתן לשתף את המידע המסווג "GREEN" עם עמיתים וארגונים שותפים בתחום, אך לא באמצעות ערוצים נגישים לציבור. אלא אם צוין אחרת, אין לשתף מידע בסיווג "ירוק" מחוץ לקהילת הגנת הסייבר
TLP: CLEAR	מקרים בהם נראה כי קיים סיכון מינימלי או לא קיים סיכון כלל בהפצה של מידע	ניתן לשתף את המידע המסווג "CLEAR" ללא הגבלה, בכפוף לשמירה על זכויות יוצרים

מקורות להרחבה:

TRAFFIC LIGHT PROTOCOL (TLP)

FIRST Standards Definitions and Usage Guidance — Version 2.0

<https://www.first.org/tlp>

Traffic Light Protocol (TLP) Definitions and Usage

<https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage>