Bundesamt
für Sicherheit in der
Informationstechnik

# Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), TLP-Version 17-11

Im Rahmen des zugrundeliegenden Informationsverbundes ist der Austausch von nichtöffentlichen und vertraulichen Informationen notwendig. Das Traffic Light Protocol (TLP) ist eine Vereinbarung zum Schutz dieser Informationen.

Das TLP regelt nicht den Schutz staatlich geheimzuhaltender Informationen.

Die vom BSI verwendete Version 17-11 des Traffic Light Protocol basiert auf dem Standard **FIRST Standards Definitions and Usage Guidance, Version 1.0** (https://www.first.org/tlp/).

Das TLP Version 17-11 unterscheidet bei der Informationsweitergabe

- den **Informationsersteller**,
- den **Verteiler** (z. B. BSI, CERTs, GÜAS, SPOCs, Verbände),
- den **Empfänger** (i. d. R. Betreiber) sowie
- **Dritte** (z. B. IT-Dienstleister), die die IT des Empfängers betreiben und hierfür in einem Vertragsverhältnis mit dem Empfänger stehen.

Die Einschränkungen zur Weitergabe betreffen Verteiler, Empfänger und die Dritten.

Das TLP dient der Schaffung von Vertrauen bzgl. des Schutzes ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung datenschutzrechtlicher Belange, Vertraulichkeit, eine Rufschädigung oder eine Beeinträchtigung der Geschäftstätigkeit zur Folge haben. Im Zweifelsfall ist in Absprache mit dem Informationsersteller zu handeln.

Durch die Unterschrift auf der TLP-Verpflichtung erklären natürliche und juristische Personen ihre Zustimmung zu den Regeln des TLP. Eine Verpflichtung stellvertretend für den eigenen Zuständigkeits-/ Verantwortungsbereich ist möglich. Werden Funktionspostfächer oder Gruppenrufnummern in der Organisation angegeben, so sind alle potenziellen Empfänger durch den Unterzeichner in dessen Verantwortung und Verwaltung auf die Einhaltung des TLP zu belehren.

## Die TLP-Stufen

### TLP:WHITE Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

### TLP:GREEN Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

### TLP:AMBER Eingeschränkte interne und organisationsübergreifende Weitergabe

Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis *Kenntnis nur, wenn nötig* weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen.

Hierfür muss er sicherstellen, dass die Dritten das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

### TLP:RED Persönlich, nur für bekannte Empfänger

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

## Allgemeine Hinweise

Die Einstufung einer mündlichen Information wird vom Urheber vorgenommen und dem Zuhörerkreis stets vor der Weitergabe mitgeteilt. Personen, die nicht auf das TLP verpflichtet sind, müssen die Besprechung für die Dauer der Weitergabe von als TLP:RED, TLP:AMBER und TLP:GREEN eingestuften Informationen verlassen.

Schriftstücke, die nach TLP eingestuft werden sollen, sind vom Informationsersteller vor Beginn des eigentlichen Informationsinhaltes auf jeder Seite des Dokuments mit dem Stichwort TLP:RED, TLP:AMBER, TLP:GREEN oder TLP:WHITE zu kennzeichnen und nur berechtigten Personen auszuhändigen.

Bei TLP:AMBER hat der Informationsersteller die Möglichkeit, die Weitergabe an Betreiber und Dritte einzuschränken. Eine Weitergabe über Dritte hinaus ist nicht erlaubt.

Beispiele für Einschränkungen sind:

- TLP:AMBER Nur organisationsinterne Weitergabe
- TLP:AMBER Nur für KRITIS-Betreiber und deren IT-Dienstleister
- TLP:AMBER Nur für privatwirtschaftliche KRITIS-Betreiber und Verbände
- TLP:AMBER Nur für staatliche Organisationen
- TLP:AMBER Nur für UP-KRITIS-Teilnehmer
- TLP:AMBER Nur für INSI-Teilnehmer
- TLP:AMBER Nur für IT-Dienstleister

Wird die Weitergabe nicht eingeschränkt, kann die Information über das BSI, SPOCs, GÜAS oder das CERT ggf. viele Betreiber erreichen.

## Einstufung und Kennzeichnung

Einstufungen sind klar zu kennzeichnen. Sie gelten in der Regel auch für Auszüge aus eingestuften Dokumenten oder Informationen. Zusätzliche Einschränkungen für den Verteilerkreis können durch den Informationsersteller ergänzend zur TLP-Stufe eingebracht werden. Die Kennzeichnung muss gut lesbar sein.

Werden mehrere Informationen unterschiedlicher TLP-Stufen zusammen gehandhabt, so sind sie entsprechend der höchsten vorliegenden TLP-Stufe zu behandeln.

Bei Nachrichten müssen Kennzeichnungen so erfolgen, dass sie für den Leser sofort deutlich erkennbar werden, z. B. als vorgestellter Text im Betreff einer E-Mail. Bei Dokumenten mit Seitenstruktur müssen die Kennzeichnungen mittig in der Kopfzeile jeder Seite erscheinen. Bei Dateien ist der Dateiname entsprechend zu ergänzen. Dies gilt auch für Dateianhänge an E-Mails oder sonstige elektronische Nachrichten. Datenträger sind zusätzlich sichtbar zu markieren.

## Weitergabe an nicht genehmigten Empfängerkreis

Sollte eine Weitergabe an einen durch die Einstufung nicht genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete in Zukunft nur noch Informationen der Stufe TLP:WHITE.

Eingestufte Dokumente (außer TLP:WHITE) dürfen weder manuell noch automatisiert auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort Dritten zugänglich sind.

## Vervielfältigung

Die Vervielfältigung von TLP:AMBER- und TLP:RED-Informationen muss auf das unbedingt notwendige Maß beschränkt werden. Vervielfältigungen sind genauso zu behandeln wie Originaldokumente einschließlich ihrer Kennzeichnung, Aufbewahrung, Weitergabe und Vernichtung.

## Aufbewahrung

Informationen der TLP-Stufen TLP:RED oder TLP:AMBER sollten in der Regel verschlüsselt aufbewahrt werden. Papierdokumente der TLP-Stufen TLP:AMBER oder TLP:RED müssen in einem verschlossenen Behältnis aufbewahrt werden.

## Elektronische Übertragung

Informationen der TLP-Stufen TLP:RED und TLP:AMBER müssen in der Regel bei elektronischer Übertragung angemessen verschlüsselt werden.

## Vernichtung, Löschung und Aussonderung

Datenträger, auf denen Informationen der TLP-Stufen TLP:AMBER oder TLP:RED gespeichert wurden, müssen vor Aussonderung sicher gelöscht oder – bevorzugt – irreversibel physisch vernichtet werden. Papierdokumente der TLP-Stufen TLP:AMBER oder TLP:RED müssen in geeigneten Aktenvernichtern vernichtet werden.

## Kompromittierung von Informationen

Bereits beim Verdacht auf Kompromittierung von Informationen (Verlust usw.) sind umgehend der Informationsersteller und das BSI zwecks Schadensminimierung über den Sachverhalt zu informieren.