SEC-10-01-S
State CIO Adopted: Dec. 10, 2024
TSB Approved: Dec. 10, 2024
Sunset Review: Dec. 10, 2027

WaTech
Washington Technology Solutions

Replaces:
Incident Communications Policy
Appendix 143a
December 10, 2014

TRAFFIC LIGHT PROTOCOL STANDARD

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"

1. **The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information for cybersecurity alerts, events, and incidents is shared with the correct audience. TLP is for communications and not data classification. SEC-10 Incident Response Policy requires communications based on the Enterprise Incident Response Plan.**

2. **TLP employs colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s). TLP designations at Washington state agencies are derived from the Cybersecurity and Infrastructure Security Agency's Traffic Light Protocol (TLP) Definitions and Usage.**

    a. TLP:Red

        i. When should it be used? Situations when information cannot be effectively acted upon without significant risk to the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only.

        ii. How should it be shared? Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

    b. TLP:Amber+Strict

        i. When should it be used? When information requires support to be effectively acted upon, yet carries a risk to privacy, reputation, or operations if shared outside of the organization.

ii. How should it be shared? Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.

c. TLP:Amber

i. When should it be used? When information requires support to be effectively acted upon, yet carries a risk to privacy, reputation, or operations if shared outside of the organization(s) involved.

NOTE: TLP:AMBER+STRICT limits the information to a single organization, whereas TLP:AMBER allows a broader distribution of the information to more than one specific organization.

ii. How should it be shared? Recipients may share TLP:AMBER information with members of their own organization, other organizations, clients or other partners on a need-to-know basis to protect their organization(s) and prevent further harm.

d. TLP:Green

i. When should it be used? Circumstances in which information is useful to increase awareness within their wider community.

ii. How should it be shared? Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside the cybersecurity or cyber defense community.

e. TLP:Clear

i. When should it be used? When information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

ii. How should it be shared? Recipients may share this information without restriction. Information is subject to standard copyright laws and rules.

3. **If a recipient needs to share the information more widely than indicated by the original TLP designation, they must first obtain explicit permission from an authorized representative of the original source.**

4. **All communications must include the TLP color in capital letters in the following format: (i.e., TLP:RED, TLP:AMBER + STRICT, TLP:AMBER, TLP:GREEN, or TLP:CLEAR).**

    a. TLP-designated email correspondence must indicate the TLP color of the information in the subject line and the body of the email prior to the designated information.

    b. TLP-designated documents must indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color must be 12-point type or greater.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-10 Incident Response Policy.
3. Traffic Light Protocol (TLP) Definitions and Usage.
4. NIST Cybersecurity Framework CSF 2.0 Mapping:
    - GOVERN.RISK MANAGEMENT STRATEGY (GV.RM-05): Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
    - IDENTIFY.IMPROVEMENT (ID.IM-04): Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.
    - RESPOND.INCIDENT RESPONSE REPORTING AND COMMUNICATION (RS.CO-03): Information is shared with designated internal and external stakeholders
    - RECOVER.INCIDENT RECOVERY COMMUNICATION (RC.CO-04): Public updates on incident recovery are shared using approved methods and messaging.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.

PROPOSED DEFINITION

Organization: Under the Traffic Light Protocol (TLP), an organization refers to a group of individuals who share a formal affiliation and are governed by the same organizational policies. This group can be as large as all members of an information-sharing entity, though it is rarely broader than that. An organization may consist of a single agency or a combination

of affected agencies, such as WaTech. Additional agencies may also be included depending on the specifics of the cybersecurity alert, event, or incident.