APCERT POLICY – INFORMATION SHARING AND HANDLING

The Asia Pacific Computer Emergency Response Team (**APCERT**) community recognises the importance of information sharing to better protect the Asia-Pacific region from malicious cyber activities. Secure handling of information is necessary to maintain trust and confidence within the APCERT community which, in turn, facilitates greater sharing.

APCERT has adopted the Traffic Light Protocol (**TLP**) an internationally recognised set of designations used to ensure that sensitive information is shared appropriately.

This document provides guidance on sharing and handling information within APCERT and is applicable to the APCERT community.

The APCERT seeks to build a cyber resilient region. Information sharing increases the region's awareness and visibility of the cyber threat landscape and builds trust and confidence amongst members.

When sharing and handling information, the APCERT community adheres to TLP as defined by the Forum of Incident Response and Security Teams (**FIRST**) (see *FIRST Standards Definitions and Usage Guidance – Version 2.0* (www.first.org/tlp). This policy should be read in conjunction with advice on the FIRST website.

Definitions

The **Traffic Light Protocol (TLP)** is a set of designations used to ensure information is shared with the appropriate audience.

The TLP uses five labels to indicate expected sharing boundaries to be applied by the recipient(s).

TLP:RED	= Not for disclosure, restricted to individual recipients only.
TLP:AMBER+STRICT	= Limited disclosure on a need-to-know basis, restricted sharing to the organisation only.
TLP:AMBER	= Limited disclosure on a need-to-know basis, restricted to participants' organisations and their constituency.
TLP:GREEN	= Limited disclosure, restricted to the community.
TLP:CLEAR	= Unlimited disclosure.

The APCERT community must adhere to this policy and use the TLP designations as defined by FIRST.

An **organisation** is the group who share a common affiliation by formal membership and are bound by common policies set by the organisation. Within the APCERT, an organisation is the named member or partner.

Constituencies are people or entities that receive cybersecurity services from an organisation.

APCERT Community refers to all APCERT members including Operational Members, Corporate and Liaison Partners.

Community responsibility

The APCERT message sender and owner of the information determines the TLP designation.

APCERT community members have the responsibility to maintain internal records when they have shared, make a request to on-share or receive TLP:RED and TLP:AMBER/TLP:AMBER+STRICT information from other APCERT Members and Partners.

Records should include the requestor, approver, any conditions, and details about the recipient.

Sharing relevant information via email

A TLP designation is required when sharing relevant information within the APCERT community.

Relevant information includes:

- The exchange of data, information, and strategies for effective cybersecurity incident response;
- The exchange of threat response data and incident handling information; and
- Other categories of cybersecurity related information as mutually determined by the participants.

When applying a TLP designation to an email:

- The TLP designations must be formatted in accordance with the FIRST Standards Definitions and Usage Guidance;
- Everything within the email, including any attachments, must be treated in accordance with the TLP designation; and
- Where appropriate, APCERT Members and Partners should also apply the appropriate encryption and/ or signature to the email.

Documents and Presentations

APCERT documents and presentations must contain a TLP designation in the header and footer and formatted in accordance with the FIRST Standards Definitions and Usage Guidance.

Handling of Unmarked Material

Unmarked material must be treated as TLP:AMBER+STRICT. Recipients should revert to the sender for the correct TLP designation.