APCERT POLICY ON INFORMATION SHARING AND HANDLING

Introduction

APCERT Operational Members and APCERT Partners must adhere to APCERT's policy on Information Sharing and Handling. The APCERT community recognises the importance of sharing information to better protect the Asia-Pacific region from malicious cyber activity. Trust and confidence is vital when sharing information. Appropriately assigning TLP designations and handling information builds and maintains trust and confidence within the APCERT community and strengthens cooperative and collaborative efforts to prevent and mitigate malicious cyber activity.

Policy

Introduction

- When sharing and handling information, the APCERT community adheres to the Traffic Light Protocol (TLP) as defined by the Forum of Incident Response and Security Teams (FIRST) – see *FIRST Standards Definitions and Usage Guidance – Version 1.0* (www.first.org/tlp).
- The TLP is a set of designations used to ensure information is shared with the appropriate audience.
- The TLP uses four colors to indicate expected sharing boundaries to be applied by the recipient(s). The four colors are red, amber, green and white.

TLP:RED	= Not for disclosure, restricted to participants only.
TLP:AMBER	= Limited disclosure, restricted to participants' organizations.
TLP:GREEN	= Limited disclosure, restricted to the community.
TLP:WHITE	= Disclosure is not limited.

Note: Please refer Appendix A for detailed TLP descriptions and usage guidance.

Traffic Light Protocol

- APCERT Operational Members and APCERT Partners must adhere to this policy and use TLP designations as defined by FIRST (TLP:RED, TLP:AMBER, TLP:GREEN and TLP:WHITE).

An 'Organization'

- For the purposes of defining an organization within the APCERT community, an organization is the named Member or Partner, or in the case of a national government CERT/CSIRT, an organization is defined as the national government of that economy.

Responsibility for assigning correct TLP designations and protections

- The APCERT message sender and owner of the information determines the TLP designation.
- It is the sender's responsibility to apply appropriate security protections when sending information to other APCERT Members and Partners.

Emails

- APCERT Members and Partners are encouraged to apply a TLP designation when emailing others within the APCERT community.
- If applying a TLP designation to an email:
    - The TLP designations should be displayed at the beginning of the email subject line and in the body of the email.
    - The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.
    - Everything within the email, including any attachments, must be treated in accordance with the TLP designation.
    - Where appropriate, APCERT Members and Partners should also apply the appropriate encryption and/or signature to the email.
    - It is recommended that the definition of the TLP designation be placed in emails so there is no doubt as to what the recipient is allowed, or expected to do with the information.

Documents and Presentations

- It is best practice that official APCERT documents and APCERT presentations contain a TLP designation in the header and/or footer.
- TLP designations must be formatted in accordance with the FIRST Standards Definitions and Usage Guidance.
- The TLP color on black background must appear in capital letters and in 12 point type or greater.
- It is advisable to right-justify TLP designations.
- It is recommended that the definition of the TLP designation be placed in documents so there is no doubt as to what the recipient is allowed, or expected to do with the information.

Maintaining Records

- All APCERT Members and Partners have a responsibility to maintain internal records of when they have shared TLP:RED and TLP:AMBER information to other APCERT Members and Partners.
- All APCERT Members and Partners have a responsibility to maintain internal records of when TLP:RED and TLP:AMBER information is received from other APCERT Members and Partners.
- All APCERT Members and Partners have a responsibility to maintain internal records of when they make a request to another APCERT Member and Partner to further share TLP:RED or TLP:AMBER information.
- Records should include who made the request, who approved the request, any conditions, and details about who the information was shared with.

TLP:RED [Not for disclosure, restricted to participants only]

- This designation is reserved for the most sensitive information and in most instances would be shared bilaterally.
- Face-to-face communication is highly recommended.
- Email should only be used in exceptional circumstances and must be encrypted and signed.
- TLP:RED information *must not* be shared with anyone else without the *explicit* permission from the originating APCERT Member or Partner.
    - At times an APCERT Member or Partner may seek to provide received information to an outside party or constituent in order to take some form of action or to mitigate or remediate an incident.
    - Received TLP:RED information can only be communicated further with the explicit permission of the originating APCERT Member or Partner. In seeking permission you must detail who you seek to share with, why, and how the information will be protected from further dissemination.
    - Only the originator of the information can approve further sharing and they can also specify conditions for use, such as the distribution method.
    - Face-to-face communication should be used when communicating TLP:RED information about a compromised organization to that compromised organization.
- At all times recipients of information must understand and adhere to the restrictions of TLP:RED. It is the responsibility of the sharing party to ensure the receiver understands any restrictions on the information.

TLP	Description	APCERT Usage	APCERT Handling
RED	**Not for disclosure, restricted to participants only** FIRST Definition: Use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	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. Sharing beyond the recipient: At times an APCERT Member or Partner may seek to provide received TLP:RED information to an outside party or constituent in order to take some form of action or to mitigate or remediate an incident. If a recipient wants to share TLP:RED information more widely, they must obtain explicit permission from the original source.	Data securing mechanism: Face-to-face is highly recommended. Encrypted and signed email may be used in exceptional circumstances. Face-to-face communication should be used when communicating TLP:RED information about a compromised organization to that compromised organization.

TLP:AMBER [Limited disclosure, restricted to participants' organizations]

- Encrypted and signed email is recommended for communication within the APCERT community.
    - TLP:AMBER information *can be shared within your organization* without the need to first seek permission from the originator.
- TLP:AMBER information *must not* be shared with anyone outside your organization without the *explicit* permission from the originating APCERT Member or Partner.
    - Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
    - Sources should consider stating up front in the original communication if there are additional CERT clients who they permit to see the TLP:AMBER information, specifically where a CERT client may need to know the information to protect themselves or prevent further harm. Where such permission is given upfront, all parties must be made aware of the TLP:AMBER restrictions and comply with the TLP:AMBER usage and data handling rules outlined in this policy.
- At times an APCERT Member or Partner may seek to provide received information to an outside party or constituent in order to take some form of action or to mitigate or remediate an incident.
    - Received TLP:AMBER information can only be communicated beyond your organization with the explicit permission of the originating APCERT Member or Partner. In seeking permission you must detail who you seek to share with, why, and how the information will be protected from further dissemination.
    - Only the originator of the information can approve further sharing and they can also specify conditions for use, such as the distribution method.
    - Face-to-face communication should be used when communicating TLP:AMBER information about a compromised organization to that compromised organization.
- At all times recipients of information must understand and adhere to the restrictions of TLP:AMBER. It is the responsibility of the sharing party to ensure the receiver understands any restrictions on the information.

TLP	Description	APCERT Usage	APCERT Handling
AMBER	**Limited disclosure, restricted to participants' organizations.** FIRST Definition: Use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	Recipients may only share TLP:AMBER information with members of their own organization. Sharing beyond your organization: At times an APCERT Member or Partner may seek to provide received TLP:AMBER information to an outside party or constituent in order to take some form of action or to mitigate or remediate an incident. If a recipient wants to share TLP:AMBER information more widely than their own organization, they must obtain explicit permission from the original source.	Data securing mechanism: Appropriate encryption and signature is recommended. Face-to-face communication should be used when communicating TLP:AMBER information about a compromised organization to that compromised organization.

TLP:GREEN [Limited disclosure, restricted to the community]

- Face-to-face communication or encryption is not required.
- Emails should be signed.
- TLP:GREEN information can be shared within your organization and with your constituents without the need to first seek permission from the originator.
- TLP:GREEN information must not be circulated via publicly accessible channels like a website.
- Internal APCERT administrative communications should be designated TLP:GREEN.

TLP	Description	APCERT Usage	APCERT Handling
GREEN	**Limited disclosure, restricted to the community.** FIRST Definition: Use TLP:GREEN when information is useful for the awareness of all participating APCERT Members, Partners and their constituents as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information widely within the APCERT community as well as with peers within the broader community or sector, but not via publicly accessible channels. Sharing Publicly If a recipient wants to share TLP:GREEN information publicly they must obtain explicit permission from the original source.	Data securing mechanism: Signed email. TLP:GREEN information may not be released outside of the community and cannot be publicly published or posted on the Internet. TLP:GREEN should be used for APCERT administrative matters.

TLP:WHITE [Disclosure is not limited]

- TLP:WHITE information can be distributed without restriction and if required placed on the internet (subject to any copyright restrictions).
- APCERT's publicly accessible information, such as the APCERT Annual Report, must be designated TLP:WHITE.

TLP	Description	APCERT Usage	APCERT Handling
WHITE	**Disclosure is not limited.** FIRST Definition: Use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. All information on APCERT's website is designated TLP:WHITE.	Data securing mechanism: Nil.

Appendix A - Example of a TLP:AMBER email:

FROM: AP-CERT-TEAM-1

TO: APCERT-TEAM-2

SUBJECT: **[TLP:AMBER] help to shut down domain**

* PGP Signed: 09/01/2018 at 3:44:48 PM

TLP:AMBER

Hello Members of Team 2,

Team 1 has become aware of information related to a domain hosting malicious software in your jurisdiction.

Information is included as an attachment to this message. We would like your help in having the servers hosting the domain cleaned and/or the site shut down.

Best regards,

Team 1.

TLP Handling Instructions:

TLP:RED = Not for disclosure, restricted to participants only.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

TLP:GREEN = Limited disclosure, restricted to the community.

TLP:WHITE = Disclosure is not limited.

Refer www.first.org/tlp for further information on the Traffic Light Protocol.

* end PGP SIG BLOCK

FAQs

What are my responsibilities as the originator of a report I want to share with the APCERT community?

As the Originator, you determine the TLP designation of the material. This is based on the level of assistance the recipient will require for the information to be acted upon as well as potential impacts on a party's privacy, reputation or operations.

What are my responsibilities as the recipient of a report as a member of the APCERT community?

As a recipient of TLP material, you are responsible for adhering to the designation assigned by the Originator which determines how you handle and share the information.

TLP:RED

I have received TLP:RED material but I need to pass this information to another agency to respond to the incident. What should I do?

Firstly, you need to obtain permission from the Originator. You need to send a request outlining the following information:

- Who you seek to share the material with.
- Why you need to share the information.
- How the information will be protected from further dissemination.

If you receive permission to share the material, it is your responsibility to adhere to any additional conditions applied to the dissemination of the material by the Originator, and ensure that the recipient of the material understands the restrictions on the information.

Once I have received permission from the originator to share TLP:RED information, how should I communicate material about a compromised organisation to that organisation?

This information should be communicated face-to-face. This is because the malicious actor may have visibility of the victim's systems.

I am sharing TLP:RED material with an APCERT Member about a compromised organisation within their economy. Can I approve the passage of the material to this organization proactively?

Yes. This is the preferred approach as it reduces the time it will take to communicate the information to the compromised organization. The APCERT Member recipient will be aware of sharing and handling restrictions, and will know the requirement to ensure the recipient within the compromised organization handles the material appropriately.

TLP:AMBER

Can I share TLP: AMBER material with other people within my organization?

Yes. You do not need to seek permission to share TLP:AMBER material with someone from your organization. For the purposes of defining an organization within the APCERT community, an organization is the named Member or Partner, or in the case of a national government CERT/CSIRT, an organization is defined as the national government of that economy.

What do I need to do to share received TLP:AMBER material with someone outside of my organization?

You need to obtain permission from the Originator. You need to send a request outlining the following information:

- Who you seek to share the material with.
- Why you need to share the information.
- How the information will be protected from further dissemination.

If you receive permission to share the material, it is your responsibility to adhere to any additional conditions applied to the dissemination of the material by the Originator, and ensure that the recipient of the material understands the restrictions on the information.

Maintaining Records

What records do I need to keep when I am sending TLP:RED and TLP:AMBER information?

When you send information at TLP:RED and TLP:AMBER it is your responsibility to maintain an internal record of who you share the information with. This is useful for your own auditing purposes.

It is advisable to record requests made by other Members and Partners to share your information, including who made the request, who they wanted to share the information with, your response, and any limitations you placed on the dissemination of the material.

What records do I need to keep when I am receiving TLP:RED and TLP:AMBER information?

When you receive information at TLP:RED and TLP:AMBER it is your responsibility to maintain an internal record of who you received the information from.

If you are requesting permission to share the information outside your organization (in line with TLP sharing requirements), it is advisable to record these requests. You should include the response to your request, who authorised the material to be shared and any limitations placed on the dissemination of the material, who you then shared the material with, and an acknowledgment that the recipient was informed of the TLP handling requirements. It is useful to record this for your own auditing purposes.