APCERT
Asia Pacific Computer Emergency Response Team

# APCERT Information Classification Policy

## Introduction

The APCERT Information Classification Policy is based on the Traffic Light Protocol (TLP) used widely by the international CSIRT community and has been adapted for APCERT requirements.

APCERT gratefully acknowledges the work conducted by other CSIRTs which first developed this protocol to facilitate trusted information exchange between CERTs and key stakeholders in their jurisdictions. Specific mention should be made of Trusted Introducer and NISCC https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf.

This APCERT policy is provided to APCERT members to:

> build trust and confidence that sensitive information will be handled appropriately by APCERT members by allowing APCERT recipients to better understand the sensitivity and/or restrictions which may apply to some types of information; and through increased trust and confidence, enable more effective and useful communication and assistance to occur between APCERT teams.

Ultimately it is the APCERT message sender and owner of the information that determines the information classification/handling. In the absence of any TLP, the default is to assume that the TLP AMBER applies, unless the sender/owner confirms otherwise.

Against each TLP classification, we have included suggested mechanisms to provide confidentiality and integrity protection. These are guidelines only for the APCERT sender to implement if they wish to do so. In practice, it may not always be possible to maintain confidentiality protection, if the information needs to be passed to a trusted third party on a “need-to-know” basis. For example, when an APCERT team receives an AMBER communication asking for assistance with a malware hosting site in the jurisdiction of the recipient APCERT team, and the recipient APCERT team then needs to communicate with an external ISP that does not have a PGP key to facilitate encryption of email between the APCERT team and the ISP, then it would not be possible to maintain encryption to all third parties who need to respond to resolve the incident. It would be expected that the recipient APCERT team still be able to communicate to the ISP without the use of encryption to achieve the desired objective of the communication – i.e. to mitigate existing harm/attack.

## Instructions

APCERT members should include the TLP classification in the email subject field. Members should also apply the appropriate encryption and/or signature to the email.

APCERT members may also wish to include the explanatory meanings of the relevant TLP classification within the body of the message so there is no doubt as to what the recipient is allowed, or expected to do with the information. It is recommended that the definition of the classification level be copied into the email.

# APCERT Information Classification Policy

An **example** of an AMBER Email would be:

FROM: AP-CERT-TEAM-1

TO: APCERT-TEAM-2

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

* PGP Signed: 09/06/2012 at 3:44:48 PM

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: AMBER***

*AMBER information is intended for specific APCERT members with a view to limited disclosure on a strict* ***"need to know basis" within your respective organisations and/or constituencies*** *in order to:*

- *assist in the protection of the recipient's ICT systems; or*
- *contact an affected / third party which has the capacity to directly mitigate an attack.*

* end PGP SIG BLOCK

# APCERT Information Classification Policy

## How to classify new information derived from information previously distributed according to an APCERT TLP classification

When an APCERT team uses information received through an APCERT mailing list or from APCERT members and derives new information related to the original information, the APCERT team that has derived the new information must classify and treat the newly derived information with the same or higher TLP classification as the original information.

For example, Team A sends information to the APCERT mailing list about an incident that it classifies as AMBER, requesting assistance from all APCERT teams in relation to the incident. Team B investigates the incident further and derives new information about the incident. In handling the derived information, Team B must classify and treat the derived information either as AMBER (the same as the original information); or RED (higher than the original TLP classification). Team B can only distribute, release or publish the derived information according to the appropriate TLP classification.

| TLP | Description | APCERT usage (examples) |
|---|---|---|
| **RED** | **For recipients only – no further disclosure**<br>Information intended for specific APCERT members only. Not for distribution beyond the recipient APCERT members.<br>If the information needs to be extended outside of the intended group, explicit authorisation in writing is needed from the document/message owner.<br>**Data securing mechanism:** Encrypted and signed (if possible) | **Example 1 -** Team C advises Teams B and D about a software security vulnerability in a proprietary system that is not public and for which there is no patch.<br>**Comment 1 -** The information is provided to Teams B and D for their information only; they are not permitted to pass the information to any other party until the affected vendor makes a public announcement.<br>**Example 2** – There is a need to update APCERT operational documents. All members are requested to provide recommendations.<br>**Comment 2** – The SC sends an email to the apcert-teams list. The communication should be restricted to these recipients. |

# APCERT Information Classification Policy

| | | |
|---|---|---|
| **AMBER** | **Limited disclosure**<br>Information intended for specific APCERT members with a view to limited disclosure on a strict “**need to know basis**” **within their respective organisations and/or constituencies** in order to:<br>• assist in the protection of the recipient’s ICT systems; or<br>• contact an affected / third party which has the capacity to directly mitigate an attack.<br>The latter may include contacting ISPs, domain name registrars or other networks within the recipient’s economy or jurisdiction.<br>If the information needs to be extended outside of the intended group, explicit permission is needed from the document/message owner.<br>**Data securing mechanism:** Encrypted and signed (if possible) | **Example 1** - There is a C&C server located in economy X that is conducting a DDOS botnet attack on a network in economy Y. APCERT Team Y asks APCERT Team X to help shut down the domain and/or host to help mitigate the attack.<br>In order to assist with this request Team X needs to contact a domain name registrar in economy X which the C&C is using and also to contact the ISP where the host is located to access copies of log files etc.<br>**Comment 1** - Under AMBER, Team X is permitted to contact the appropriate third parties within its economy (X) who have the ability to directly mitigate the attack but is not permitted to disclose this information to anyone else.<br>**Example 2** - Team B advises Teams X and Y about a software security vulnerability in a proprietary SCADA system which has limited use which is not public and for which there is no patch.<br>The information is provided to Teams X and Y for limited disclosure only for the purposes of protecting affected ICT systems.<br>**Comment 2** - Under AMBER, Team X and Y are only permitted to pass the information to those few network owners or operators within their economies (or constituents) that use this software and are directly affected by this bug so they can take other precautions until a patch is released. |

| | | |
|---|---|---|
| **GREEN** | **Community wide**<br>Information that can be shared **widely within the APCERT member community and/or APCERT teams' constituencies among trusted parties**; but which cannot be publicly published or posted on the Internet.<br>**Data securing mechanism:** signed | **Example 1 -** Team J has received a report of a security incident from an organisation within the transport industry in its economy/constituency. The incident relates to a concern about a possible network intrusion and some sample log file entries are provided with a question whether similar activities have been seen elsewhere by other teams in the economy or other teams in the APCERT region.<br>With the approval of the affected transport organisation, Team J removes details of the affected network but passes information about the unusual log file entries to a range of APCERT teams, in order to ask whether similar log activity has been detected by their constituents.<br>**Example 2 -** APCERT Team S has a list of malicious URLs that are serving malware and/or include redirections to malware hosting sites. The list is useful to check against network log files to determine whether any internal hosts have made connections to these malicious sites as a way to detect potentially compromised internal hosts.<br>Team S provides the information to other APCERT teams so these teams may in turn, distribute the information, if they wish, to trusted parties within their economies or constituents.<br>**Comment -** Under GREEN, APCERT teams that receive this message are permitted to disseminate the information request broadly within their economy or constituency to trusted parties to enquire whether the similar log activity has been detected elsewhere.<br>Recipients of GREEN information are not permitted to disclose the information publicly by posting on the internet or other publicly accessible forum/mailing list. |

| | | |
|---|---|---|
| **WHITE** | **Not restricted**<br>Information is intended for immediate public distribution to all APCERT members and their constituents, subject only to copyright and any restrictions or rights noted in the information.<br>**Data securing mechanism:** signed | **Example 1** APCERT produces an annual report which is posted on the APCERT web site. It includes information provided by individual APCERT members.<br>This information is classified as WHITE. |
| **DEFAULT** | Any information received from an APCERT member by another APCERT member that is not classified in accordance with the TLP must be treated as AMBER, unless otherwise advised in writing by the APCERT member that owns /disseminated the information. | |