APCERT Member & Partner Categories Policy

Introduction

1. The Asia Pacific Computer Emergency Response Team (APCERT) is a forum for national and non-national Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs) within the Asia Pacific region to foster information sharing and collaboration on cyber security. APCERT has relationships with a wide range of organisations within the Asia Pacific region and around the globe.

APCERT Operational Members

2. Operational Members form the core of the APCERT community – they are the national and leading CSIRTs and CERTs from across the Asia Pacific region[1] that meet the following criteria, as stated in the Operational Framework.

3. APCERT Operational Members must:

- be a CSIRT or CERT from an Asia Pacific economy, which performs the function of a CSIRT or CERT on a full time basis;
- be a leading or national CSIRT or CERT within its own economy;
- be not-for-profit and/or wholly or partly government funded;
- have established policies, practices and procedures for operating a CSIRT or CERT within its economy and have experience in CSIRT operations including incident handling and cyber threat and vulnerability monitoring and advice;
- have a broad responsibility and capability for disseminating information and coordinating incident response across and/or among sectors within its economy;
- make contributions to the Asia Pacific CSIRT/CERT community; and
- advise the APCERT SC, within a reasonable time period, if at any time it cannot meet the above criteria.

4. Operational Members are expected to be active participants in APCERT to the greatest extent possible, namely with contributions to the Annual Report, participation in the Annual General Meeting (AGM) and the Annual Drill.

5. Operational Members have full access to all APCERT information sharing and collaborative platforms[2] and initiatives and are eligible to participate in any (or all) of the APCERT Working Groups[3]. Operational Members also have the right to vote on APCERT operational matters and to stand for the Steering Committee and other elected positions after holding membership for one year. Each Operational Member has one (1) vote.

[1] The Asia Pacific region refers to the Asia Pacific Network Information Centre's (APNIC) geographic boundaries of 60th degree parallel (longitude). A list of the economies within the Asia Pacific region is listed on the APNIC web site. See: http://www.apnic.net/about-APNIC/organization/apnics-region.

[2] Such platforms include, for example, the closed APCERT Operational Membership email list, the APCERT Wiki (hosted by MyCERT) and the APCERT Data Exchanger (hosted by CNCERT/CC).

[3] As at November 2015, the APCERT Working Groups are: Cyber Green, Information Sharing, Membership, Policy Procedures & Governance, Training and TSUBAME.

APCERT Partners

6. Separate to APCERT Operational Members, APCERT has three partnership categories – *"Liaison Partner", "Strategic Partner"* and *"Corporate Partner",* as stated in the Operational Framework. APCERT Partners do not have any voting rights but may observe and provide feedback on APCERT operational matters. Partners receive a standing invitation to the APCERT Annual Conference.

Liaison Partners

7. There are some CERTs/CSIRTs with which APCERT has – or would like to have – a formal relationship but which are not eligible for operational membership. These organisations include national and non-national CERTs/CSIRTs from outside the Asia Pacific region, and CERTs/CSIRTs that do not yet meet Operational Member joining requirements.

8. An APCERT Liaison Partner must:

- be a full-time national CSIRT or CERT which is either
    a. ineligible for operational membership because it is located outside the APCERT region, or
    b. is potentially capable of becoming an Operational Member but does not yet meet Operational Member requirements;
- be not-for-profit and/or wholly or partly government funded;
- share APCERT's vision to help create a safe, clean and reliable cyber space through global collaboration and is willing to partner with APCERT to achieve this vision; and
- agree and be able to protect information provided by APCERT and its members appropriately in line with the Traffic Light Protocol (TLP) 4.
- be approved by the SC under an MoU with APCERT; and
- advise the SC, within a reasonable time period, if at anytime it cannot meet the above criteria.
- The exchange of official contact details and the potential exchange of CERT-to-CERT operational information are at the core of the Liaison Partner relationship. Liaison Partnership allows a two-way flow of points of contact and information to support CERT/CSIRT operations. It is a mutual partnership based on the vision of helping create a safe, clean and reliable cyber space through global CERT-to-CERT collaboration.

9. As equivalent CERT organisations, APCERT Liaison Partners receive a standing invitation to attend the APCERT Annual General Meeting and Conference. They are also eligible to be invited to participate in the APCERT annual Drill and some APCERT Working Groups, at the discretion of the Working Group convenor and APCERT Steering Committee. Liaison Partners are also able to pursue other collaborative activities of mutual interest with APCERT, including the exchange of tools and techniques, cyber security exercises and capacity building activities such as training. The exchange of information between APCERT and its Liaison Partners occurs in accordance with the TLP.

[4] APCERT's use of the Traffic Light Protocol is codified in its Information Classification Policy, which is available at http://www.apcert.org/documents/index.html.

Liaison Partners

A Liaison Partner is an individual national CSIRT/CERT that principally or completely operates outside the geographic boundaries of APCERT and is not-for-profit and/or wholly or partly government funded, or are potentially capable of becoming an Operational Member but do not yet meet Operational Member requirements. Such entities become Liaison Partners because they wish to establish a formal relationship with APCERT and official points of contact for incident response, as well as to pursue information sharing and other collaborative activities with APCERT and its members.

Strategic Partners

10. Strategic Partners are government or not-for-profit organisations—not CERTs/CSIRTs—that provide cyber security or internet-related services. Strategic Partners include entities such as Internet registries, law enforcement agencies, network operators and collaborative cyber security groups.

11. An APCERT Strategic Partner must:

- be a government or not-for-profit organisation that provides internet-related services (e.g. domain registry or internet address allocation) or carries out particular cyber security functions (e.g. multilateral national and leading CERT groupings, law enforcement or other cyber security function);
- share APCERT's vision to help create a safe, clean and reliable cyber space through global collaboration and be a willing to partner with APCERT to achieve this vision;
- agree and be able to protect information provided by APCERT and its members appropriately in line with the TLP;
- be sponsored by three (3) existing APCERT Operational Members;
- be approved by the SC under an MoU with APCERT; and
- advise the APCERT SC, within a reasonable time period, if at anytime it cannot meet the above criteria.

Corporate Partners

12. There are a range of commercial cyber security-related entities that wish to formally support the operation and activities of APCERT. Such entities have the opportunity to join APCERT as a Corporate Partner.

13. APCERT Corporate Partners must:

- be a cyber security related commercial entity that, regardless of its regional base and organizational structure, will support and contribute to the APCERT operation;
- be able to support CSIRT/CERT functions;
- comply with the APCERT Engagement with Service Providers and Corporate Entities Policy;
- be sponsored by three (3) existing APCERT Operational Members;
- be approved by the SC under an MoU with APCERT; and
- advise the APCERT SC, within a reasonable time period, if at any time it cannot meet the above criteria.

14. The core element of the Corporate Partner relationship with APCERT is that they have ability to contribute to APCERT operations and activities. This contribution or support can come in the form of in-kind assistance such as training, seminars or presentations at APCERT events. It can also involve financial support, for example the APCERT Fellowship Program which provides assistance to selected APCERT members to attend the APCERT Annual General Meeting (AGM) and Conference, sponsoring the APCERT AGM and Conference or other related events.

15. Corporate Partners are also able to share information and support other collaborative cyber security activities and initiatives with APCERT and its members, including capacity building. In addition, they are eligible to participate in some APCERT Working Groups, at the discretion of the Working Group convenor and the APCERT SC.

APCERT Member and Partner Approval Process

APCERT Operational Members

16. To apply for operational membership a potential member must:

- Obtain one (1) APCERT Operational Member sponsor, who will be required to submit a Sponsor Report;
- complete an Operational Membership Application Form and submit it to the APCERT Secretariat;
- agree to a site visit by an APCERT Operational Member if required. The need for a site visit on the potential member will be at the discretion of the APCERT Steering Committee.
- be approved by unanimous APCERT SC decision.

17. New Operational Members are recorded in the minutes of the relevant SC meeting, which are circulated to all APCERT members. Applicants will be advised of the application outcome by the APCERT SC. If successful, the APCERT Secretariat will also notify all members of the new Operational Member via email.

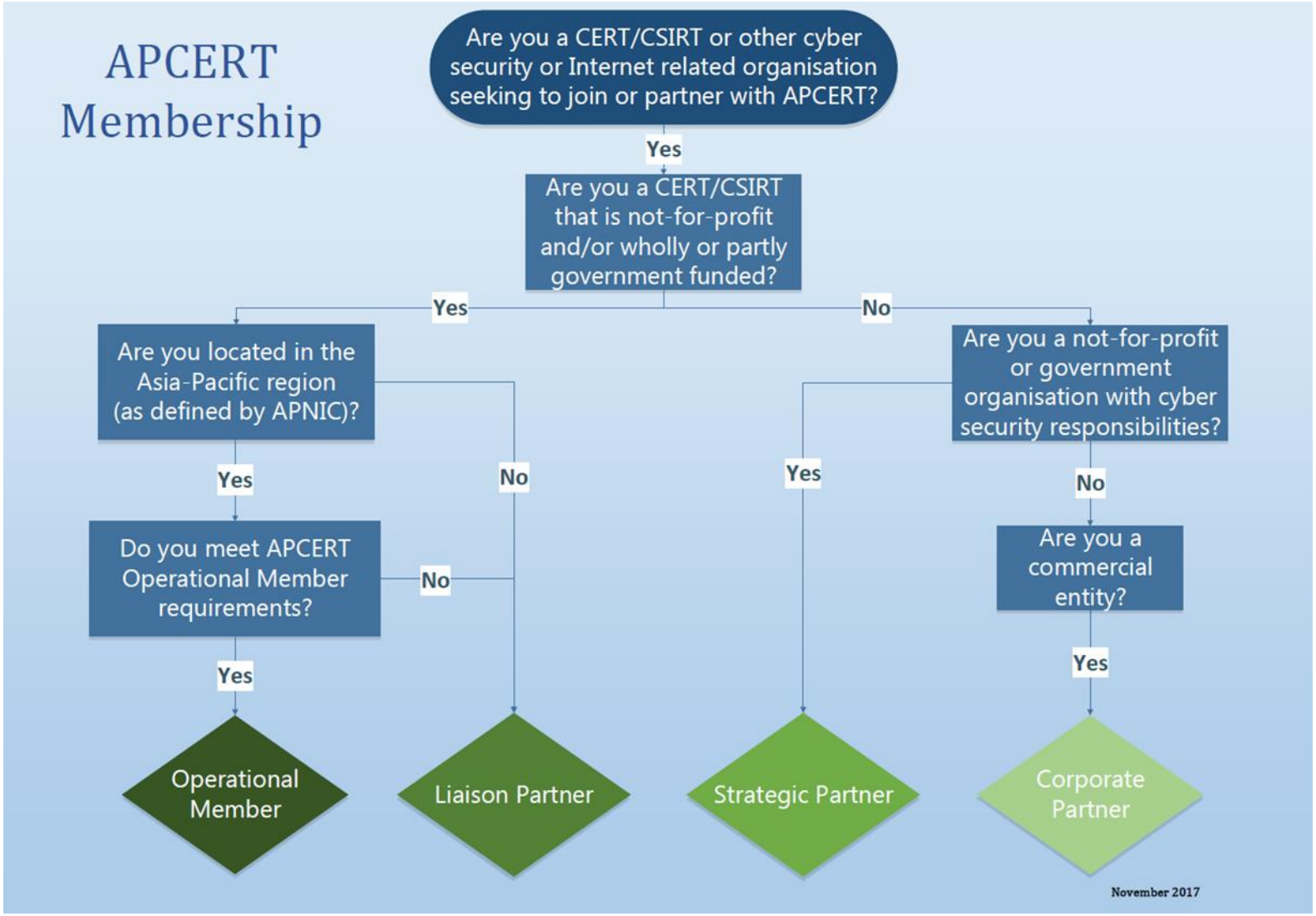
18. APCERT Operational Members are also published on the APCERT public website.

APCERT Partners

19. A potential APCERT Partner can be proposed by any APCERT member, or a potential partner can apply through the APCERT Secretariat. A potential partner must:

- be sponsored by three (3) existing APCERT Operational Members;
- be approved by the SC under an MoU with APCERT. The MoU must be agreed unanimously by the SC and signed by the SC Chair on behalf of APCERT. The MoU must be countersigned by the partner organisation's designated and authorised authority within that organisation. Where applicants and SC are unable to sign the MoU in-person, due to the inability to travel, with the unanimous approval of the APCERT SC, digital signing of the document will be allowed.

20. APCERT Partners are also published on the APCERT public website.


APCERT Membership
Are you a CERT/CSIRT or other cyber security or Internet related organisation seeking to join or partner with APCERT?
Yes
Are you a CERT/CSIRT that is not-for-profit and/or wholly or partly government funded?
Yes
No
Are you located in the Asia-Pacific region (as defined by APNIC)?
Yes
No
Do you meet APCERT Operational Member requirements?
No
Yes
Operational Member
Liaison Partner
Are you a not-for-profit or government organisation with cyber security responsibilities?
Yes
No
Strategic Partner
Are you a commercial entity?
Yes
Corporate Partner
November 2017

APCERT OPERATIONAL MEMBERS

APCERT Member			
Relationship	**Criteria**	**Contribution**	**Benefits**
Operational Member	An APCERT Operational Member must: 1. be a CSIRT or CERT from an Asia Pacific economy, which performs the function of a CSIRT or CERT on a full time basis; 2. be a leading or national CSIRT or CERT within its own economy; 3. be not-for-profit and/or wholly or partly government funded; 4. have established policies, practices and procedures for operating a CSIRT or CERT within its economy and have experience in CSIRT operations including incident handling and cyber threat and vulnerability monitoring and advice; 5. have a broad responsibility and capability for disseminating information and coordinating incident response across and/or among sectors within its economy; and 6. make contributions to the Asia Pacific CSIRT/CERT community.	Mandatory: • Contribution to the Annual Report. Required to the extent possible: • Participation in the AGM and • Participation in the APCERT Drill. Highly Desirable: • Participation in APCERT Working Groups • Contributions through the sharing of cyber security information.	All: • Access to shared information, including SC Meeting Minutes. • Incident response assistance, including POC arrangements. • Voting rights on APCERT operational matters (after holding membership for one year). • Eligibility to stand for Steering Committee and other elected positions (after holding membership for one year). • Participation in APCERT initiatives – e.g. TSUBAME Working Group, ADE and APCERT wiki. • Participation in other APCERT activities (including training and capacity building).

APCERT PARTNER MEMBERSHIP CATEGORIES

APCERT Partners			
Relationship	**Criteria**	**Contribution**	**Benefits**

Liaison Partner MoU	An APCERT Liaison Partner:
	• Is a full-time national CSIRT or CERT which is either
	  ○ ineligible for operational membership because it is located outside the APCERT region, or
	  ○ is potentially capable of becoming an Operational Member but does not yet meet Operational Member requirements;
	• is not-for-profit and/or wholly or partly government funded;
	• shares APCERT's vision to help create a safe, clean and reliable cyber space through global collaboration and is willing to partner with APCERT to achieve this vision; and
	• agrees and is able to protect information provided by APCERT and its members appropriately in line with the TLP.
		Mandatory:
		• Provide Liaison Partner POC for incident response.
		Highly Desirable:
		• Contributions through the sharing of cyber security information with APCERT.
		• Contribution to APCERT activities (e.g. training or other events)
		• Collaboration with APCERT on other CERT-to-CERT activities.
			All:
			• Standing invitation to the APCERT AGM and Annual Conference.
			• Access to APCERT POC arrangements.
			• Eligibility for APCERT Working Group membership, at the discretion of the Working Group convenor and the Steering Committee.
			• Eligibility to participate in the APCERT annual Drill, at the discretion of the Drill Organising Committee and the Steering Committee.
			• Access to information from APCERT members, at the discretion of members and/or the Steering Committee.
			• Opportunities to collaborate with APCERT on other CERT-to-CERT activities, at the discretion of the Steering Committee.

APCERT Partners			
Relationship	**Criteria**	**Contribution**	**Benefits**
Strategic Partner MoU	An APCERT Strategic Partner: • is a government or not-for-profit organisation that provides internet-related services (e.g. domain registry or internet address allocation) or carries out particular cyber security functions (e.g. multilateral national and leading CERT groupings, law enforcement or other cyber security function) • shares APCERT's vision to help create a safe, clean and reliable cyber space through global collaboration and is willing to partner with APCERT to achieve this vision; and • agrees and is able to protect information provided by APCERT and its members appropriately in line with the TLP.	Optional: • Collaboration with APCERT and its members on regional and/or global cyber security initiatives and activities • Information sharing with APCERT and its members • Contribution to APCERT capacity building activities.	All: • Standing invitation to APCERT Annual Conference. Optional (where applicable): • Collaboration with APCERT and its members on regional and/or global cyber security initiatives and activities • APCERT support for regional capacity building activities • Information sharing with APCERT and its members.
Corporate Partner MoU	An APCERT Corporate Partner: • is a cyber security-related commercial entity that, regardless of its regional base and organizational structure; • is able to support CSIRT/CERT functions; • shares APCERT's vision to help create a safe, clean and reliable cyber space through global collaboration and is willing to partner with APCERT to achieve this vision; and A Corporate Partner must comply with the APCERT Engagement with Service Providers and Corporate Entities Policy.	Mandatory: • Contribute to APCERT activities (e.g. training, sponsorship, presentations). Optional (where applicable): • Information sharing with APCERT and its members • Provide operational POC for incident response • Provide financial support to APCERT activities (e.g. Fellowship program).	All: • Standing invitation to APCERT Annual Conference • Access to APCERT network for information sharing and incident response assistance (including access to Corporate Partner email distribution to APCERT Operational Members) • Eligibility for some APCERT Working Groups (at WG convenor's discretion) Optional (where applicable): • Speaker slot at APCERT Annual Conference. • Opportunities for corporate sponsorship • Other collaborative activity opportunities.