

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

The purpose of the Asia Pacific Computer Emergency Response Team (APCERT) is to encourage and support cooperation among Computer Security and Incident Response Team (CSIRT) and Computer Emergency Response Team (CERT) organizations in the Asia Pacific region.

1 Background

With the rapid development of the Internet, many Asia Pacific economies are increasingly dependent on public network applications such as online services, including banking and finance, business and government. The protection of critical information infrastructure in the region is central to political stability, economic prosperity and regional security in the Asia Pacific.

Malicious cyber activity against critical information infrastructure is increasing in frequency, sophistication and scale. This growing threat in the Asia Pacific region requires a collaborative approach, with the various CSIRT and CERT organizations taking the lead role with the full support from their respective governments.

To address this need, the APCERT was established with a focus on operational capability and readiness to prevent and mitigate malicious cyber activity.

1.1 History of APCERT

In March 2002, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) invited the leading CSIRTs and CERTs from Asia Pacific economies to attend the Asia Pacific Security Incident Response Coordination Conference (APSIRC). The aim of APSIRC was to improve working relationships among CSIRTs and CERTs in the region.

The key outcome of the APSIRC meeting was the decision to form the APCERT, consisting of 15 CSIRTs and CERTs from 12 Asia Pacific economies, as the vehicle for regional cross border cooperation and information sharing in mitigating cyber threats.

In February 2003, the members of the APSIRC meeting accepted the APCERT agreement and elections were held for the positions of Chair and Secretariat, and the membership of the Steering Committee (SC). In February

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

2005, during the APCERT Annual General Meeting (AGM) in Kyoto, Japan, the position of Deputy Chair was created and elected.

The APSIRC set out the initial goals and objectives upon which the APCERT was established. The APCERT vision was revised in 2011 to reflect the broadened perspective of the group and its members.

2 Mission

The APCERT will maintain a trusted contact network of cyber security experts in the Asia Pacific region to improve the region's awareness and competency in relation to cyber security incidents through:

1. enhancing Asia Pacific regional and international cooperation on cyber security;
2. jointly developing measures to mitigate large-scale or regional network security incidents;
3. facilitating information sharing and technology exchange on cyber security and threats among its members;
4. promoting collaborative research and development on subjects of interest to its members; and
5. assisting other CSIRTs and CERTs in the region to conduct efficient and effective computer emergency response.

3 APCERT Operational Membership

APCERT Operational Membership is open to all suitably qualified CSIRTs and CERTs in the Asia Pacific region. The Asia Pacific region refers to the Asia Pacific Network Information Centre's (APNIC) geographic boundaries of 60th degree parallel (longitude).¹

APCERT Operational Members, in seeking and accepting APCERT Operational membership, must agree to support the objectives of the APCERT, respect the information handling caveats for information received from APCERT Operational Members and, where possible, provide assistance to APCERT Operational Members.

¹ 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>.

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

Operational Members are eligible to vote on APCERT operational matters after one (1) year of membership. Each Operational Member has one (1) vote. Operational Members have the right to stand for SC and other elected positions after holding membership for one (1) year.

There is an expectation that Operational Members will be active participants in APCERT to the extent possible, namely with contributions to the APCERT Annual Report and participation in the AGM and APCERT Drill which are the key elements of APCERT activities. As such, Operational Members are required to contribute to the APCERT Annual Report and should also participate in the AGM and/or APCERT Drill. Further information on Operational Member benefits and expectations can be found in APCERT's Member and Partner Categories Policy.

3.1 Operational Member Criteria

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;
6. make contributions to the Asia Pacific CSIRT/CERT community; and
7. advise the APCERT SC, within a reasonable time period, if at anytime it cannot meet the above criteria.

3.2 Operational Member Application Process

To apply for operational membership a potential member must:

1. obtain one (1) APCERT Operational Member sponsor, who will be required to submit a Sponsor Report;
2. complete an Operational Membership Application Form and submit it to the APCERT Secretariat;

Asia Pacific Computer Emergency Response Team (APCERT)
OPERATIONAL FRAMEWORK

3. agree to a site visit by an Operational Member; and
4. be approved by unanimous APCERT SC decision.

4 APCERT Partners

Separate to APCERT Operational Members, APCERT has three partnership categories – “*Liaison Partner*”, “*Strategic Partner*” and “*Corporate Partner*”.

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. Further information can be found in APCERT’s Member and Partner Categories Policy.

4.1 Liaison Partner Criteria

An APCERT Liaison Partner must:

1. 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;
2. be not-for-profit and/or wholly or partly government funded;
3. 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;
4. agree and be able to protect information provided by APCERT and its members appropriately in line with the APCERT Information Classification Policy; and
5. advise the SC, within a reasonable time period, if at anytime it cannot meet the above criteria.

4.2 Strategic Partner Criteria

An APCERT Strategic Partner must:

1. 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);

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

2. 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;
3. agree and be able to protect information provided by APCERT and its members appropriately in line with the APCERT Information Classification Policy; and
4. advise the APCERT SC, within a reasonable time period, if at anytime it cannot meet the above criteria.

4.3 Corporate Partner Criteria

An APCERT Corporate Partner must:

1. be a cyber security related commercial entity that, regardless its regional base and organizational structure, will support and contribute to the APCERT operation;
2. be able to support CSIRT/CERT functions;
3. 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;
4. agree and be able to protect information provided by APCERT and its members appropriately in line with the APCERT Information Classification Policy;
5. agree and be able to protect information provided by APCERT and its members appropriately in line with the APCERT Information Classification Policy;
6. comply with the APCERT Engagement with Service Providers and Corporate Entities Policy; and
7. advise the APCERT SC, within a reasonable time period, if at anytime it cannot meet the above criteria.

4.4 Partner Application Process

To apply for any partner category a potential partner must:

1. be sponsored by three (3) existing APCERT Operational Members;
2. complete an Partner Application Form and submit it to the APCERT Secretariat;
3. be approved by unanimous APCERT SC decision; and
4. sign an MoU with APCERT.

OPERATIONAL FRAMEWORK

5 Review or Revocation of Membership/Partnership or Change of Category

The APCERT SC may review the continued eligibility and suitability of Operational Members or other Partners at any time. If the APCERT SC is of the opinion that a member/partner no longer meets the membership eligibility requirements, or is otherwise unsuitable for APCERT membership, it may recommend that APCERT revoke or change that membership/partnership.

The decision to change or revoke operational membership is subject to the approval of:

1. a two-thirds quorum of the APCERT Operational Members with voting rights during the GM; or
2. if votes are to be cast by email, by more than half of the total number of APCERT Operational Members with voting rights.

The decision to change or revoke partners under MoU is taken by the SC in accordance with the provisions of the MoU.

6 Code of Conduct

6.1 Duty of Members and Partners

All APCERT Operational Members and Partners have a duty to abide to the Code of Conduct. Breach of Code of Conduct may result in sanctions.

6.2 Investigation of Suspected Breach, Decision and Penalty

6.2.1

The Steering Committee may investigate a suspected breach of Code of Conduct of any Operational Member or Partner at any time. If the Steering Committee is of the opinion that a material breach has occurred, a compliance notice may be served to the member/partner.

6.2.2

The compliance notice must:

- State the channels of communication the notice was served by;
- State the occurrence of the breach and possible adverse effects;

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

- State the opinion and rationale of the Steering Committee in issuing the compliance notice;
- State the actions and timeline the member/partner may pursue to remediate the breach;
- State the actions and timeline the Steering Committee may pursue if the member/partner may not comply or respond to the notice;
- Allow reasonable time for the member/partner to respond to the notice; and
- Include a copy of the appeal mechanism as per section 6.3, the member/partner may pursue.

6.2.3

If the member/partner fails to reply to the compliance notice within the reasonable time or continue to breach the Code of Conduct, the Steering Committee may serve a second compliance notice to the member/partner, following the same format as the first notice.

6.2.4

If the member/partner fails to reply to the second compliance notice or continue to breach the Code of Conduct, the Steering Committee may lodge to apply sanctions on the member/partner. These sanctions may include revocation of partial or full permission of access to APCERT resources such as the mailing list. The sanction would not include the revocation of membership / partnership or change of membership / partnership category which is governed by section 5.

6.2.5

The Steering Committee must inform the member/partner of the intended sanctions in a sanction notice and reserves the right to notify all operational members about the breach.

6.2.6

Sanctions applied take effect not earlier than 30 days after the sanction notice is issued. The Steering Committee specifies the length of sanction period in the sanction notice, or else, a default period of 12 months applies. The maximum sanction period is 12 months from the effective date of sanction. The renewal of sanctions requires the issuance of another sanction notice by the Steering Committee.

OPERATIONAL FRAMEWORK

6.3 Appeal Mechanism

6.3.1

An appeal may be made to the Steering Committee against the effect of any compliance notice or sanction notice, not later than 30 calendar days after the notice was served.

6.3.2

If an Appeal is called, the Steering Committee will set up an Appeal Panel composing of:

- One (1) Appeal Panel Chair who is an Operation Member not being part of the Steering Committee,
- Four (4) Appeal Panel Members, two (2) from the Steering Committee and two (2) from Operational Members not being part of the Steering Committee.

6.3.3

The Appeal Panel may revisit the decision of the Steering Committee and decide to accept all sanctions, or suspend, in totality or partially any sanctions before they take effect. The decision of the Appeal Panel is final.

7 Organization

The APCERT comprises:

- 1 . General Meeting (GM) – consisting of all APCERT Operational Members. The GM will be convened by the Steering Committee and attended by representatives of APCERT Operational Members. The GM will be the principle vehicle for defining and agreeing overall directions of APCERT. A GM will only be convened if at least half of APCERT Operational Members with voting rights are present at the meeting. At a minimum, the GM will be convened annually, known as the Annual General Meeting (AGM).

APCERT Partners under MoU may be invited to attend appropriate sessions of the GM.

The Steering Committee (including Chair and Deputy Chair) and the Secretariat will be elected at an AGM. The AGM will also be used to

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

accept and approve reports from the Steering Committee and other APCERT members as required.

2. Steering Committee (SC) – consisting of a maximum of seven (7) representatives elected by more than half of a quorum of APCERT Operational Members with voting rights during the AGM. Only Operational Members may nominate to the SC. SC Members are appointed for two-year terms and are responsible for the overall management of the APCERT. Each half of the SC Members will be elected on alternate years to ensure continuity of SC membership.

The Steering Committee will hold teleconferences at least every two (2) months, or more often as required, and will meet in person at least once a year. SC meetings will only be convened if 5/7 of the SC members are present. Any proposals discussed by the SC will be approved by the SC with a minimum of 4/7 potential votes.

3. Chair – SC member elected by the SC to chair the Committee. The chair will be appointed for a term of one (1) year and will be responsible for the coordination of the SC. A member may only serve as Chair for a maximum of four (4) consecutive terms.
4. Deputy Chair – SC member elected by the SC as Deputy Chair of the Committee. The Deputy Chair will share the responsibilities of the Chair, including deputizing for the Chair and providing assistance as required. The term is for one (1) year. A member may only serve as the Deputy Chair for a maximum of four (4) consecutive terms.
5. Secretariat – an Operational Member elected by the SC to provide secretariat support to the Committee. The Secretariat is the first point of contact for the APCERT, and maintains the records of membership information, provides general guidance for potential members, serves as an administrative point for APCERT and maintains the web site and e-mail lists. The Secretariat's tasks will be approved by the SC. The Secretariat has no authority to make decisions on behalf of the APCERT. The Secretariat serves a term of two (2) years.
6. Working Groups – refer 'APCERT Working Group Guidance' and see APCERT website for current list of APCERT Working Groups.

For further information about APCERT election procedures please refer to:

OPERATIONAL FRAMEWORK

- Procedures for Election of APCERT Steering Committee Members, Chair, Deputy Chair and Secretariat.

8 Point of Contact (POC) Arrangements

The APCERT POC Arrangements provide a framework for sharing information about serious and time critical cyber threats, vulnerabilities or incidents by APCERT members within the region.

Where there is more than one (1) Operational Member from an economy, that economy will propose one (1) of those members to be the POC for that economy.

APCERT POC members should give priority to requests for assistance made under the APCERT POC Arrangements.

It is an obligation of all members which are the POCs for their economy to ensure that their contact details are kept up-to-date. The POCs are listed at the APCERT secure website. Changes to the POCs details should be submitted to the Secretariat.

For further information about these procedures see:

- APCERT POC Arrangements Policy
- Guidelines for APCERT POC Arrangements
- APCERT POC Form

9 Eligibility for Liaison Partners and Strategic Partners to Participate in APCERT POC Arrangements

Liaison Partners are eligible to participate in the APCERT POC Arrangements. Strategic Partners may also be considered for inclusion in the APCERT POC Arrangements on a case by case basis, subject to SC approval.

Liaison and Strategic Partners engaging with APCERT in its POC Arrangements agree to abide by the APCERT POC Arrangements policies and guidelines where applicable to the Participating External CERTs/CSIRTs.

For further information about these procedures see:

Asia Pacific Computer Emergency Response Team (APCERT)
OPERATIONAL FRAMEWORK

- APCERT Guidelines for CSIRTs Outside AP Region.

10 Mailing Lists

The APCERT operates a range of mailing lists. To prevent these lists from being used by spammers, members should not publicly disclose the existence of these lists and their contents.

Other email aliases may be established from time to time to manage specific short-term projects or issues.

Members are encouraged to use the generic contact email address of other members when communicating directly with them.

For further information about these procedures see:

- APCERT Mailing List Procedures.

11 Activities and Focus Areas

In accordance with the APCERT's stated goals and objectives, the APCERT and its elected representatives will undertake activities in the following broad areas.

11.1 Process and Structure

The SC will establish operating and management parameters, including²:

1. APCERT member policies and procedures;
2. means of secure communications for the APCERT members;
3. policies, procedures and guidelines that allow information to be shared to the fullest possible extent among APCERT members;
4. guidelines for receiving and handling reports of computer attacks from within and external to the region; and
5. a web site to publish relevant information and documents.

² This list is not exhaustive and the items are not in any particular order of importance. The Steering Committee is to deliberate on the actual work to be done and their prioritization.

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

11.2 Outreach and Assistance

Develop initiatives to assist other CSIRTs and CERTs in the region that do not have ready access to the necessary technical skills, knowledge and experience to conduct efficient and effective cyber security and incident response.

11.3 Information Sharing

The APCERT will put in place mechanisms for information sharing among its members, including:

1. an Early Warning System to facilitate fast and efficient information sharing among APCERT members;
2. a mechanism to share information on cyber threats in the Asia Pacific region; and
3. cyber security and incident response workshops and seminars.

11.4 Research and Development

Conduct joint research and development on subjects of interest to APCERT members and to produce situation reports on cyber security and incident response issues across the Asia Pacific economic community.

11.5 Annual Conference

Organize an annual conference to raise awareness on cyber security and incident response, and sharing of information.

The annual conference will be hosted by a volunteer Operational Member in September–November each year. The APCERT Secretariat will seek nominations approximately 12 months prior to the next conference. Operational Members may also express their interest in hosting a conference directly to the Secretariat. The SC will approve the conference host. Where multiple nominations are received to host the conference, the SC will conduct a majority vote. In the event of a tie, the SC Chair will cast the deciding vote.

11.6 Drill Exercise

1. The APCERT will, at least annually, conduct a drill for its members. The SC will announce the timing of a new drill via the apcert-teams list.

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

2. It is desirable for all members to participate in these drills. However, Operational Members are required to participate unless written notification of non-participation has been given and accepted by the SC before the drill event.

12 Process for Changing APCERT Policies and Procedures

APCERT members may propose additions or changes to APCERT policies and procedures as they appear in this document. The proposed changes must be submitted in writing to the SC with details of the existing policy or procedure (if applicable), and reason for the proposed change or addition. The SC will consider the proposal and will either accept, reject or amend the proposal and consult with the Operational membership as required.

Any proposals to amend, alter or otherwise change the Operational Framework will be submitted for approval by at least two-thirds of a quorum of Operational Members with voting rights during the GM or, if votes are to be cast by email, by more than half of the total number of APCERT Operational Members with voting rights. If approved the proposed changes become part of the Operational Framework.

13 SC Minutes and Reporting to APCERT Members

The APCERT SC will, at a minimum, keep a record of the APCERT SC decisions in the form of Minutes of Meeting.

The SC minutes will be available to Operational Members only.

Each year the Chair will submit a report to the AGM Closed Session on the activities of the SC for the previous 12 months.

Each year, the APCERT shall prepare an Annual Report. This report will include individual member reports prepared and submitted by APCERT members and the Chair's report. The Annual Report will be available to the public.

14 Summary of the APCERT Operational Framework

The APCERT Operational Framework constitutes the main source of information on how the APCERT operates and its mission and general activities. A number of other documents exist and should be read in conjunction with the Operational Framework. The diagram below outlines the supplementary information.

This document will be updated as required when new APCERT policies and procedures are included or modified.

This document was based on the original Proposal for Establishing an Asia Pacific Computer Emergency Response Team (APCERT) which formed the basis of the first APCERT charter and terms of reference but has since been updated to reflect changes and additions to the original terms of reference.

This document, with the exception of the section on APCERT email aliases can be made available on the APCERT web site. www.apcert.org.

Asia Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK

Appendix 1: Operational Framework, Policies and Procedures

