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 the cooperation between 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 now increasingly dependent on public network applications such as online banking, online stock trading, e-business, e-government and e-customs. The protection of the various national information infrastructures that make up this new and emerging Asia-Pacific e-economy is critical to the region's political and economic stability and security. The need to protect these critical national information infrastructures is also urgent.

Attacks on information infrastructures are increasing in frequency, sophistication and scale. This growing threat in the Asia-Pacific region requires a collaborative approach with the various CERT and CSIRT organisations taking the lead role with the full support from their respective governments.

To address this urgent need the Asia-Pacific Incident Response Teams (APCERT) was established. APCERT has an operational focus.

History of APCERT

As an initiative of JPCERT/CC, the leading CERTs and Computer Security Incident Response Teams (CSIRTs) from economies in the Asia Pacific region were invited to attend an Asia-Pacific Security Incident Response Coordination (APSIRC) meeting in Japan in March 2002 to discuss improved working relationships between CSIRT neighbours across international borders.

A key outcome from the APSIRC meeting was the decision to form APCERT as the vehicle for regional cross border cooperation and information sharing. A working group was formed which used a consultative process to forge an agreement for the 15 CERT teams from the 12 Asia Pacific economies that agreed to establish APCERT.

In February 2003, the APCERT agreement was accepted by attendees of the APSIRC meeting and elections were held for the positions of Steering

Committee, Chair and Secretariat. During the AGM in Kyoto in February 2005, the position of Deputy Chair was created and a team elected.

Many of the goals and objectives of APSIRC firmly established and became the legacy upon which APCERT is built.

2. Mission

APCERT will maintain a trusted contact network of computer security experts in the Asia-pacific region to improve the regions' awareness and competency in relation to computer security incidents through:

1. enhancing Asia-Pacific regional and international cooperation on information security;

2. jointly developing measures to deal with large-scale or regional network security incidents;

3. facilitating information sharing and technology exchange, including information security, computer virus and malicious code, among its members ;

4. promoting collaborative research and development on subjects of interest to its members;

5. assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response;

6. providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

3. Membership

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

[1] A list of the economies within the Asia-Pacific region are listed on the APNIC web site. See: http://www.apnic.net/info/faq/apnic_faq/about_apnic.html

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

APCERT has two membership levels – *full members* and *general members*. Applicants for APCERT membership must be accepted as a general member for at least one year before being eligible to apply as a full member.

3.1 Full Member

To be eligible for full membership, a CERT or CSIRT must demonstrate that it:

- has established policies, practices and procedures for operating a CSIRT within its economy and has experience in CSIRT operations including incident handling and computer threat and vulnerability monitoring and advice; and
- is a leading or national CSIRT or CERT within its own economy; and
- has broad responsibility and capability for disseminating information and coordinating incident response across and/or within sectors within its economy; and
- not-for-profit and/or is wholly or partly government funded; and
- has made contributions to the Asia-Pacific CERT/CSIRT community.

CSIRTs for commercial organisations and organisation-centric or vendor based CSIRTs or IRTs are not eligible for full membership.

Applications to join APCERT as a Full Member will be discussed and approved on a case by case basis by the Steering Committee. Full Members have the right to vote on APCERT issues and to stand for election to the Steering Committee in the General Meeting. Each APCERT Full Member will have one vote. Founding Members are considered *Full Members*.

Some full members are also the POC for their economy. One POC team is allowed per economy. The POC is responsible for disseminating time critical and serious threat and vulnerability information and coordinating incident handling for serious and time critical incidents within its own economy.

3.2 General Member

Any CERT or CSIRT from the Asia-Pacific economies which performs the function of a CSIRT on a full-time basis and which is sponsored by an APCERT full member and approved by the SC will be allowed to join as general member of APCERT. Applications to join APCERT will be discussed and approved on a case by case basis by the Steering Committee. General Members have no rights to vote nor to stand for election.

General members will be eligible to apply for full membership after serving at least 12 months as a general member. Acceptance of general members as a full member is subject to meeting the criteria for full membership.

3.3 Revocation of Membership or Change of Membership Level

The APCERT SC may review the continued eligibility and suitability of APCERT full and general members at any time. If the SC considers that a team no longer meets the membership eligibility criteria, or is otherwise considered unsuitable for APCERT membership, then the SC will put a recommendation to revoke the team's membership or to change the team's membership level to the full members. Decisions to change or revoke a team's membership or membership level is subject to approval by at least two-thirds of a quorum of full members or by a majority of full members for votes cast by email.

4. Organization

The APCERT comprises a:

1. **General Meeting (GM)** – to be convened by the Steering Committee and attended by representative of APCERT members. During the General Meeting overall directions of APCERT will be defined, election of Steering Committee members, and acceptance/approval of reports from the Steering Committee. The meeting is normally held once a year. GM will only take place if at least ½ of APCERT full members are present at the meeting.

2. **Steering Committee (SC)** – A maximum of seven (7) representatives elected by 1/2 of APCERT Full Members during the General Meeting. Appointed for a term of two (2) years and responsible for the overall management of APCERT. Half of the committee members will retire each year to ensure continuity of service.

   The Steering Committee will hold teleconferences at least every two months, or more often as required, and will meet in person at least once per year or more often when opportunities arise. SC meetings will only take place if 5/7 of the SC members are present at the meeting. Proposals discussed by the SC will be approved by the SC with a minimum of 4/7 potential votes.

3. **Chair** – a representative from the SC elected by the Steering Committee. The chair will be appointed for a term of one (1) year and will be responsible for coordination of the Steering Committee. A representative cannot serve as Chair for more than four (4) consecutive terms.

4. **Deputy Chair** – a representative from the SC elected by the Steering Committee. The Deputy Chair will share some of the responsibilities of the Chair and will provide assistance to the Chair in his/her role as APCERT Chair, as required. The term is for one (1) year. A team may only serve a maximum of four (4) consecutive terms.

5. **Secretariat** – a representative from the SC or a full member of APCERT elected by the Steering Committee. The Secretariat will provide a general contact point for APCERT, and maintain the records of Member information, provide general guidance for potential members, serve as an administrative point for APCERT and maintain the web site and e-mail lists. The Secretariat tasks will be approved by the Steering Committee. The Secretariat has no power to make decisions on behalf of APCERT.

   The term is for two (2) years.

For further information about APCERT election procedures please refer to:

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

5. Point of Contact (POC) Arrangements

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

Each economy that is a member of APCERT will propose one (1) CERT/CSIRT that is a member of APCERT to be the POC for that economy. Full members are preferred, however, in the absence of an eligible full member within an economy a general member may be a POC.

APCERT teams should give priority to requests for assistance from other APCERT teams that use the POC alias.

It is an obligation of all teams which are POCs for their economy to ensure that their contact details are kept up to date. The POCs are recorded on the restricted access POC web site (URL IS http://www.apcert.org/related/index.html). Changes to the POCs details should be submitted to Secretariat.

For further information about these procedures see:

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

Eligibility for External CSIRTs to Participate in APCERT POC Arrangements

APCERT SC will consider requests from CSIRTs outside the Asia-Pacific region to participate in the APCERT POC Arrangements. Requests will only be accepted from:

- leading or national CSIRTs outside the Asia-Pacific region which are recognised as having broad responsibility to their economy as a whole; and
- which participate in Regional POC Arrangements compatible with the APCERT POC Arrangements.

Vendor or organizational-centric CSIRTs or incident response teams are not eligible to participate in the POC arrangements. They may continue to contact individual APCERT teams through publicly advertised contacts for each team.

Sector based CSIRTs will be considered on a case by case basis.

External CSIRTs engaging with APCERT in its POC Arrangements agree to abide by the APCERT POC Arrangements policies and guidelines where applicable to the Participating External CSIRT.

For further information about these procedures see:

- APCERT Guidelines for CSIRTs Outside AP Region)

6. Mailing Lists

APCERT operates a range of mailing lists. To prevent these addresses being used by spammers, teams should not publicly advertise the existence of these addresses. See APCERT Mailing List Procedures for further details.

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

Teams are also encouraged to use the generic contact email address of individual teams to communicate directly between teams.

7. Activities and Focus Areas

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

Process and Structure

1. Steering Committee to work on establishment of operating and management parameters such as[2]:

   (i) Develop the APCERT Member policies and procedures

   (ii) Establish a means of secure communications for its members

   (iii) Establish policies, procedures and guidelines to allow information to be shared to the fullest possible extent among members

   (iv) Establish guidelines for receiving and handling reports of computer attacks from within and external to the region

   (v) Develop a web site to publish relevant information and documents

Outreach and Assistance

2. Develop initiatives to assist other CERTs and CSIRTS in the region that do not have ready access to the necessary technical skills, knowledge and experience to conduct efficient and effective computer emergency response.

Information Sharing

3. Establish an Early Warning system to make information sharing between its membership as fast and efficient as possible

4. Develop an Anti-virus Forum to share anti-virus and malicious code information in the Asia-Pacific region

5. Organize workshops and seminars relating to information security and incident response

[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.

Research and Development

6. Conduct joint research and development on subjects of interest to its members, and produce situation reports on network security and incident response issues across the Asia-Pacific economic community.

Annual Conference

7. Organise an annual conference to raise awareness on computer security incident response and trends and sharing of information.

Drill Exercise

8. 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.

9. It is a highly desirable requirement that all members participate in these drills. In particular, full members are expected to participate but if for any reason they cannot, they should advise the SC in writing in advance of the drill.

8. Process for Changing APCERT Policies and Procedures.

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

Details of proposals approved by the SC must subsequently be submitted to the remaining full members and approved by at least two-thirds of a quorum of full members during meetings or a majority of full members via email before they can be formally accepted as part of the Operational Framework and its associated documentation.

9. SC Minutes and Reporting to APCERT Membership

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

The SC minutes will be available to full members only.

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

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

10. Summary of APCERT Operational Framework

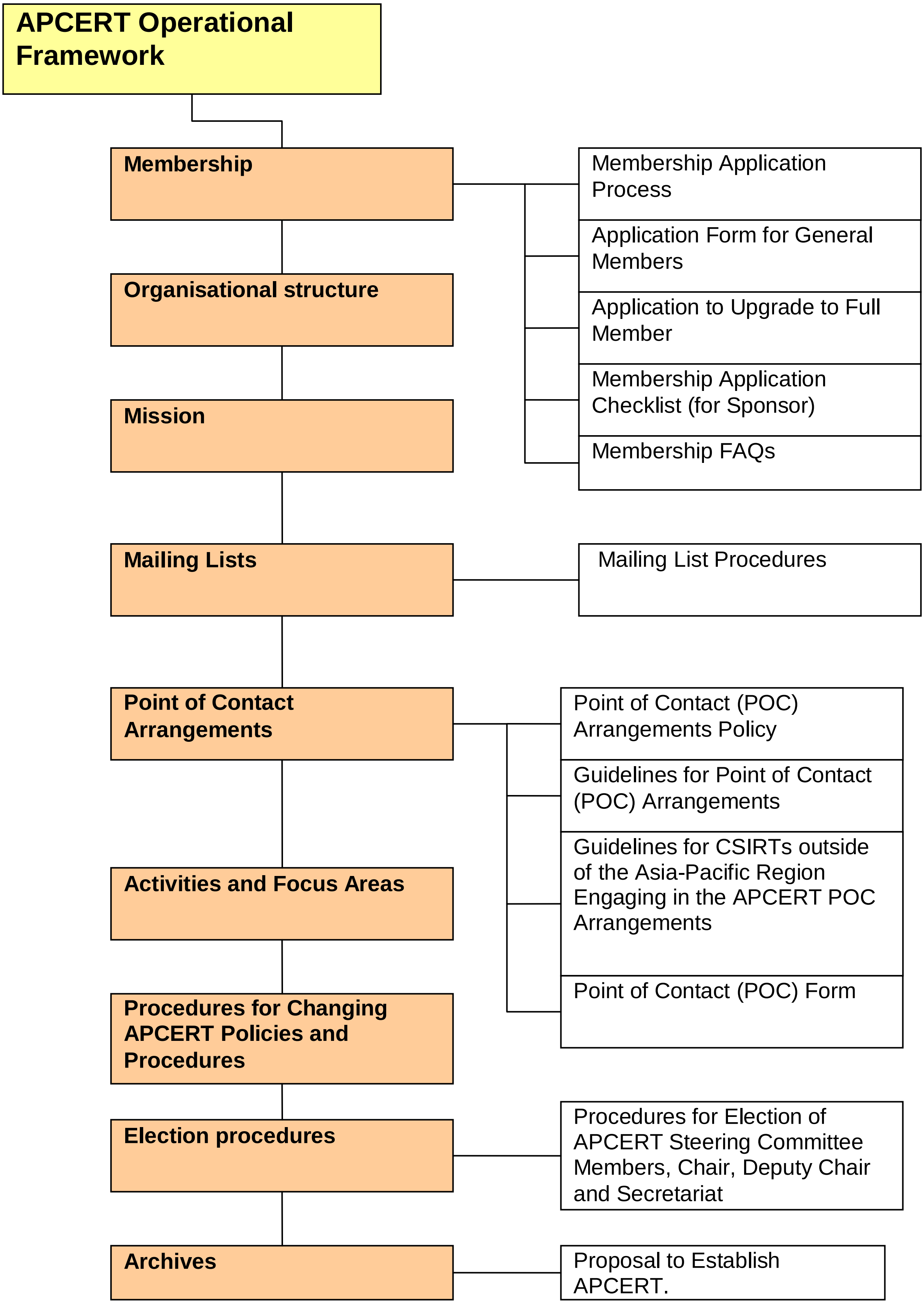
The Operational Framework constitutes the main source of information about how APCERT operates, its mission and general activities. A number of other documents exist and should be read in conjunction with the Operational Framework. The diagram below outlines supplementary information.
This document will be updated as 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 from the APCERT web site. www.apcert.org.

Asia-Pacific Computer Emergency Response Team (APCERT)

OPERATIONAL FRAMEWORK


APCERT Operational Framework
Membership
Membership Application Process
Application Form for General Members
Application to Upgrade to Full Member
Membership Application Checklist (for Sponsor)
Membership FAQs
Organisational structure
Mission
Mailing Lists
Mailing List Procedures
Point of Contact Arrangements
Point of Contact (POC) Arrangements Policy
Guidelines for Point of Contact (POC) Arrangements
Guidelines for CSIRTs outside of the Asia-Pacific Region Engaging in the APCERT POC Arrangements
Point of Contact (POC) Form
Activities and Focus Areas
Procedures for Changing APCERT Policies and Procedures
Election procedures
Procedures for Election of APCERT Steering Committee Members, Chair, Deputy Chair and Secretariat
Archives
Proposal to Establish APCERT.