**Asia Pacific Computer Emergency Response Team**

**(APCERT)**

**Application Form for an OPERATIONAL Member**

**Operational Member**

The APCERT Operational Membership is open to all suitably qualified Computer Security Incident Response Team / Computer Emergency Response Team (CSIRT / CERT) in the Asia Pacific region. In seeking and accepting the APCERT Operational membership, the entity 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.

Please fill in the form below and submit the application to the APCERT Secretariat at [apcert-sec@apcert.org](mailto:apcert-sec@apcert.org). This application needs to be digitally signed with PGP or GPG by the applying team’s APCERT Representative (apcert-rep). The Applicant will need to send the PGP public key of the team’s representative (mandatory) and team’s usage (mandatory) in a separate attachment in .asc or .txt format.

The information provided in this application form will be treated as confidential. Only APCERT personnel specific to the application process will have access to this information, except for the information marked with asterisks which will be made public through [http://www.apcert.org](http://www.apcer.org):

* Partnership type (OPERATIONAL MEMBER)
* Official team name (Item 1)
* Short Team name (Acronym) (Item 2)
* Team constituency (Item 7)
* Contact information (Item 11.1, 11.2, 11.3 and 11.4)

To qualify as an Operational Member, the entities must meet the specific criteria as outlined in the APCERT Operational Framework. Please indicate below if you meet each criterion or not :

|  |  |
| --- | --- |
| **Criterion** | **Yes/No** |
| 1. Are you a Computer Security Incident Response Team (CSIRT) / Computer Emergency Response Team (CERT) within the Asia Pacific economy, which performs the function of a CSIRT or CERT on a full time basis? | * Yes * No |
| 1. Are you a leading or national CSIRT or CERT within your own economy? | * Yes * No |
| 1. Are you not-for-profit and/or wholly or partly government funded? | * Yes * No |
| 1. Do you have established policies, practices and procedures for operating a CSIRT or CERT within your economy, and have experience in CSIRT operations including incident handling and cyber threat and vulnerability monitoring and advice? | * Yes * No |
| 1. Do you share APCERT’s vision to help create a safe, clean and reliable cyber space through global collaboration and are willing to partner with APCERT to achieve this vision? | * Yes * No |
| 1. Do you have a broad responsibility and capability for disseminating information and coordinating incident response across and / or among sectors within your economy? | * Yes * No |
| 1. Have you obtained an APCERT Operational Member Sponsor and has that sponsor conducted a site visit and completed the ‘Report for Sponsors on New Operational Members’? | * Yes * No |
| 1. Do you agree to advise the APCERT Steering Committee(SC), within a reasonable time period, if at any time you cannot meet the above criteria? | * Yes * No |

If you responded ‘Yes’ to all questions, please complete the following. If you answered ‘No’ to any of the questions, please consider applying for one of APCERT’s Partner categories.

Please provide your sponsor’s information:

(These must be APCERT Operational Members that are eligible to vote on APCERT matters)

SPONSOR 1

|  |  |
| --- | --- |
| Sponsor’s Organization: |  |
| IDD Phone/Fax: |  |
| Contact Name of Sponsor: |  |
| Contact Email: |  |

APPLICANT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Official Team Name\*: | | | |  | |
|  | Short Team Name\* (Acronym): | | | | |  |
|  | Host Organization (if the team is decentralized, list all host organizations): | | | | | |
|  |  | | | | | |
|  | Economy where the Team is located (if multiple offices exist, list all locations): | | | | | |
|  |  | | | | | |
|  | Date of Establishment: |  | | | | |
|  | Funding Model\* (check one or more) | | | | | |
|  | * Wholly Government Funded * Partially Government Funded * Subscription based * Other (please specify below) | | | | | |
|  | Other type of funding model: | | |  | | |
|  | Team Constituency\* (check one or more): | | | | | |
|  | * Economy based * Government Network * Critical Infrastructure * University based * Other (please specify below) | | | | | |
|  | Other type of constituency: | |  | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Internet Domain Name, IP Address Information and/or other characterization of the constituency: | | | | | | | |
|  |  | | | | | | | |
|  | Mission Statement: | | | | | | | |
|  |  | | | | | | | |
|  | Specify the authority given if possible. (Please explain about the relation of the authority and your constituency i.e. where your team received the authority to act as a CSIRT/CERT)): | | | | | | | |
|  |  | | | | | | | |
|  | Remarks  [Note: Please use the space below to address any issues or explanations in support of this application.] | | | | | | | |
|  |  | | | | | | | |
|  | Contact Information (The information from 11.1 through 11.4 will be made public.) | | | | | | | |
|  | * 1. **\*** Regular Phone Number (all fields below are mandatory) | | | | | | | |
|  | Time-zone (relative to GMT): | | | | |  | | |
|  | IDD Telephone number: |  | | | | | | |
|  | Days/hours of operation: |  | | | | | | |
|  | * 1. **\*** Emergency Phone Number (if different from the above “Regular Phone Number”) | | | | | | | |
|  | Time-zone (relative to GMT): | | | | |  | | |
|  | IDD Telephone number: |  | | | | | | |
|  | Days/hours of operation: |  | | | | | | |
|  | * 1. **\*** Other Communication Facilities | | | | | | | |
|  | Recommendation: “your-IRT-email-address@your.domain” | | | | | | | |
|  | Email Address (mandatory): | | |  | | | | |
|  | IDD Facsimile Number (optional): | | | | | |  | |
|  | **\*** World Wide Web Server (optional): | | | | | | |  |
|  | Postal Mailing Address (mandatory): | | | | | | |  |
|  |  | | | | | | | |
|  | APCERT representative (apcert-rep).  This person will be responsible for providing information to the sponsor and the APCERT secretariat when required during the membership application process. Once the application has been approved, this person will be responsible for keeping the teams contact information up to date and representing its team during APCERT General Meetings | | | | | | | |
|  | Name of the contact person: | |  | | | | | |
|  | Contact telephone number: | |  | | | | | |
|  | Recommendation: “apcert-rep@your.domain” | | | | | | | |
|  | Email Address (mandatory): | |  | | | | | |
|  | Aliases to be included in APCERT mailing lists  APCERT-TEAMS mailing list: apcert-teams@apcert.org  Recommendation: “apcert-team@your.domain” | | | | | | | |
|  | Email Address (mandatory): | | | |  | | | |

1. Please attach appropriate supporting documents for verification purposes.
   * National CSIRT/CERT: demonstrate government recognition as a national CSIRT/CERT.
   * Leading CSIRT/CERT: demonstrate evidence of leadership role in disseminating information and coordinating incident response across and/or among sectors within your economy.
   * Evidence of established policies for operating as a CSIRT or CERT.
   * Evidence of experience in CSIRT operations within your economy, including incident handling and cyber threat and vulnerability monitoring and advice.
2. Services

* Vulnerability analysis
* Malware analysis
* Forensic analysis
* Incident response support
* Incident response coordination
* Vulnerability response coordination

Specify available proactive services using the following list

* Announcements (intrusion and vulnerability warnings and advisories)
* Technology watch
* Security audit
* Trend and neighbourhood watch
* Configuration/maintenance of security tools
* Development of security tools
* Provision of intrusion detection services

Specify security quality management services, using the following list

* Risk analysis
* Business consulting
* Awareness building
* Training
* Product evaluation
* Provision of intrusion detection services

1. Are your PGP Key revocation certificates created and stored in a safe place? [Yes / No]

* Yes
* No