AfricaCERT Point of Contact (APOC) Guidelines.

V2: August 2019
TLP White.

The AfricaCERT establishes a Point of Contact Guidelines to ensure it has means to reach out to Members, National Point of contacts, Partners and key stakeholders for the effectiveness of its mission. The AfricaCERT POC Guidelines has been established to support information sharing within the AfricaCERT service region.

The POC Guidelines have several components:

- Member update
- National point of contact
- Partner and Other points of contact
- Additional Consideration for AfricaCERT POCs.

Part I. Member update.

1. AfricaCERT Members are required to update their membership information with AfricaCERT Secretariat at least once a year or anytime there is an important change.

2. AfricaCERT Secretariat at least every year shall reach out to Members expect Members approved that year and request update of information.

3. At the approval of a new member, the Secretariat shall reach out to the new member for point of contact information.

4. It is the responsibility of AfricaCERT members to ensure that their team information as well as their National POC information is accurate at all time and to inform AfricaCERT Secretariat.

5. Information requested during the update process

During the AfricaCERT Member update, the Secretariat shall request the following information:

a) Member POCs.

AfricaCERT Members shall provide at least two points of contact (POC) for the Member update process. One POC serves a primary contact while the others serve as secondary contacts. For each POC, the information requested is:

- Name
- Phone number if possible reachable by SMS, WhatsApp, Signal, and/or telegram
- Email … @domain
- PGP Key (Team key if applicable)

b) Special POCs consideration: National POC (Check National Point of Contact for more information).

AfricaCERT Members are also required whenever possible to notify the Secretariat if the POC serves as a National point of contact for the whole Country/Economy; this should be decided within each economy. This POC should be a leading CSIRT within

their economy that has broad responsibility and operational capacity as a whole, including among industry, vendors, ISPs and law enforcement. The Economy or National POCs should make the effort to provide means to be reachable via telephone 24 x 7, preferably one that also uses SMS technology.

Members fill the AfricaCERT POC form (africacertpocform.doc) and email it (or submit it) to AfricaCERT secretariat. In addition, the National POC designated by their economy shall fill in the AfricaCERT Nationalpocform.doc

The POC Arrangements assume that every AfricaCERT member has already established policies in place for how it will respond to requests for assistance.

AfricaCERT shall provide a single e-mail distribution list of all POCs.

All contact details for the POC arrangements shall be posted on the AfricaCERT secure website. It is the responsibility of all participating teams to ensure that the POC details are up to date at all times. This can be done by forwarding an email to the Secretariat.

Part II. National Point of Contact

Purpose

The AfricaCERT National Point of Contact (NatPOC) arrangements are designed to provide a POC for the Nation/Economy in case a member of the secretariat or an approved partner wishes to communicate information about:

a. serious and time-critical cyber security incidents and/or issues for the purposes of helping to resolve or investigate an incident; and/or
b. serious and time-critical cyber security vulnerabilities, knowledge of which is not yet in the public domain; and/or
c. serious and time-critical cyber security threats in order to provide early warning to the POC's constituents and/or to other POCs within its regional CERT/CSIRT group. An example of this is a newly discovered fast spreading Internet worm.

When there is more than one (1) Operational Member in a country/economy, there shall be one (1) team designated as the NatPOC for that economy. The nominated team shall provide POC details to the Secretariat.

The Secretariat shall reach out to the members of that economy/national to ensure that the team has the mandate to act as the national point of contact.

The Secretariat shall ensure with AfricaCERT Board of Directors the listing of the Team as NatPOC within AfricaCERT.

Requirement

The NatPOC serves as single the point of contact for economies in the AfricaCERT region.

The NatPOC are required to:

a. provide generic telephone contact numbers, e-mail addresses and PGP keys for the POC and SMS-compatible telephone numbers where possible;
b. have backup arrangements in place to support the POC arrangements;
c. provide English-speaking contacts where possible;
d. have escalation procedures in place so that immediate action can be undertaken or be able to gain appropriate authorization for action with minimal delay.

Action to be taken by the NatPOC

In responding to requests for assistance, through the POC Arrangements:

a. The POC undertakes to assist the originating reporting party to resolve a cyber-issue as fast as possible within the POC's own guidelines, powers, capabilities (including resource constraints) and legal constraints and taking into consideration its other priorities.
b. The POC undertakes to contact other parties within its constituency in order to provide the assistance required or to inform relevant parties where appropriate about the alleged incident.
c. If it is not possible to provide some or all of the assistance requested of the POC for any reasons, then the POC should inform the originating requesting party of the extent of its ability to assist, if at all.
d. It is the responsibility of the POC to establish and maintain effective contact arrangements with other CSIRT/CERT teams and other entities within their economy.
e. When an AfricaCERT NatPOC receives information about a serious and timely critical cyber issue, and the POC is able to, or is permitted to, share this information with other AfricaCERT members, then, the POC shall do so.
f. Where the original reporting party allows a NatPOC to use its discretion as to which organisations the information could be shared with, then the NatPOC should only pass sensitive information to those that it trusts to abide by the information handling caveats.

Part III. Partner and Other Point of Contact (POPC)

AfricaCERT also establishes Point of Contacts with other stakeholders within the African Internet Ecosystem such as the Law Enforcement community, domain name operators, local Internet Registries, ISP associations, Af organisations etc…

The goal is not to overshadow Members and National CSIRTs but to supplement their efforts. POPCs also serves as last resort for economies not covered by any AfricaCERT Member.

1. In general, AfricaCERT reaches out to identify organizations every year and requests an update on the point of contact.

2. While there is no formal form, AfricaCERT expects to collect the following information from POPCs:

    a. Primary and if possible, a second point of contact
    b. Name of the contacts
    c. Email address
    d. Phone or emergency contact number
    e. PGP Key

IV. Additional Consideration for AfricaCERT POCs.

1. Timeliness

In case of time sensitive cyber issue, AfricaCERT POCs shall take into consideration the urgency of the information. In addition, NatPOCs shall take into consideration the likelihood that the issue could have an immediate or imminent and widespread impact.

2. Confidentiality

In the case of restricted and confidential information being provided to a NatPOC the NatPOC should not pass information to any other third parties, even if it is permitted to do so, unless the NatPOC has a trusted relationship with the third party and only if the trusted third party agrees to abide by the information handling caveats before the information is passed.

Honoring Information Handling Caveats Imposed by the Originating Reporting Party

3. AfricaCERT POCS agree to abide by any information handling caveats imposed by the originating reporting party.

4. Where an AfricaCERT POC is permitted to communicate with third parties about the information provided by the originating reporting party, the APOC shall ensure that the recipients are aware of the information handling caveats that apply to the information, and where possible, seek their agreement to abide by them.

Breaches of Handling Caveats

5. Honoring information handling caveats is vital for AfricaCERT success to build and maintain trusted relationships. This is particularly important sharing information on issues that are not in the public domain.

6. When restricted information is disclosed it should be brought to the attention of the originating party and to who else had had access to that information. Inquiries should be made to determine if a breach occurred within their economy, and if so, how it may have occurred. If a breach is confirmed, then the relevant AfricaCERT POC should seek and provide an explanation to the affected parties and to the AfricaCERT Board.

----------END OF DOCUMENT----------