National Cybersecurity Hub Profile (South African National CSIRT)

Established according to RFC 2350

1. About this document

This document contains a description of the National Cybersecurity Hub as implemented by RFC 2350[1].

1.1. Date of last Update

This is version 1.0, published 2016/07/01.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May be Found

The current version of this document can be found at: www.cybersecurityhub.gov.za.

1.4. Authenticating this Document

The document has NOT been signed with the PGP key of the Cybersecurity Hub, The PGP key is still outstanding and will be available in Section 2.8 of this document as soon as it is finalised.

2. Contact Information

2.1. Name of the Team

Full Name: National Cybersecurity Hub.

Short Name: CSHub.

The Cybersecurity Hub is South Africa's National Computer Security Incident Response Team (CSIRT).

2.2. Address

Cybersecurity Hub
P O Box 395
Pretoria
0001
South Africa

2.3. Time zone

UTC +02

2.4. Telephone number

The Cybersecurity Hub can only be contacted by email, see Section 2.7.

2.5. Facsmile Number

CSHub can NOT be contacted by Facsimile.

[1] http://www.ietf.org/rfc/rfc2350.txt

2.6. Other Telecommunications

None available.

2.7. Electronic Mail Address

info[at]cybersecurityhub.co.za;

This is a mail alias that relays mail to all CSHub members. There is always one member on duty during business hours. This member handles all incoming mail.

2.8. Public Keys and Other Encryption Information

Encryption for secure communication is NOT supported yet.

2.9. Team Members

The information about the CSHub team members is provided on request.

2.10. Other Information

General information about CSHub can be found at www.cybersecurityhub.gov.za.

2.11. Points of Customer Contact

The preferred method for contacting the CSHub is via e-mail; e-mails will be acted upon by the officer on duty during business hours.

3. Charter

CSHub operates under the mandate of the National Cybersecurity Policy Framework (NCPF) of 2012.

3.1. Mission Statement

The mission of the Cybersecurity Hub is to be the central point of collaboration for cybersecurity incidents. The CSHub serves the South Africa cyber community through the following actions:

- Provide information and assistance in implementing proactive measures to reduce the risks of computer security incidents as well as responding to such incidents.
- Respond to computer security incidents when they occur and therefore to build confidence in the South African ICT environment.

3.2. Constituency

The CSHub constituency are South African businesses, civil society and the public.

3.3. Sponsorship and/or Affiliation

The South African government will fund the work of CSHub.

The CSHub is a non-profit entity.

3.4. Authority

The CSHub operates under the auspices of the Department of Telecommunications and Postal Services of South Africa.

4. Policies

4.1. Types of Incident and Level of Support

The CSHub is authorised to address computer security incidents which occur or threaten to occur, at its constituency (see Section 3.2). The CSHub may act upon request of one of its constituents or may act if a constituent is involved in a computer security incident.

The level of support given by CSHub will vary depending on the type, urgency and severity of the incident or issue, the size of the affected users, and the CSHub resources at the time; though in all cases some response will be made within one working day.

4.2. Cooperation, Interaction and Disclose of Information

The CSHub is mandated by the NCPF to enhance interaction, consultations and to promote a coordinated approach regarding engagements with the private sector and civil society.

All incoming information related to incidents is handled confidentially by CSHub, regardless of its priority. Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

CSHub supports the Traffic Light Protocol (TLP) for all information sharing, that is, information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately. Like other CSIRTs, the CSHub use the information provided to help solve security incidents.

4.3. Communication and Authentication

The Use of PGP/ GnuPG encryption is currently being investigated within the Hub with the view to implementation in the near future. In cases where there is doubt about the authenticity of information or its source, CSHub reserves the right to authenticate this by any (legal) means.

5. Services

Below is a list of services and functions offered by the CSHub:

Service	Functions
Alerts and warnings	Gather and receive information. Disseminate information. Notify specific parties or constituents.
Announcements	Gather and receive information. Disseminate information. Notify specific parties or constituents.
Awareness building	Organise workshops for different constituencies on various cybersecurity topics.
Incident handling	Triage: Establish focal point for receiving information. Handling: Identify involved parties. Announcement: Generate information to the constituency on how to react to incident.
Incident response support	Identify and provide support to victim and involved parties.
Security related-information dissemination	Gather and receive information. Provide central portal for distribution of information. Set up mailing list.

6. Incident Reporting

According to the National Cybersecurity Policy Framework all public and private institutions as well as the South African society have to report their cybersecurity incidents to the CSHub website: www.cybersecurityhub.gov.za

7. Disclaimer

None.