MINISTRY
COMMUNICATIONS AND DIGITAL TECHNOLOGIES
REPUBLIC OF SOUTH AFRICA

TLP: WHITE

CSHUB-CSIRT DESCRIPTION

According to RFC2350

CSIR, Meiring Naude Road, Brummeria, Pretoria, 0001, South Africa; cshubcsirt@cybersecurityhub.gov.za

Table of Contents

CSIR, Meiring Naude Road, Brummeria, Pretoria, 0001, South Africa; cshubcsirt@cybersecurityhub.gov.za

1 DOCUMENT INFORMATION

DOCUMENT TITTLE	CSHUB-CSIRT description according to RFC2350
DOCUMENT NUMER	2020-01-23-RFC2350-1.4
DOCUMENT CATEGORY	Governance and Management
DOCUMENT VERSION NUMBER	1.4
EFFECTIVE DAE	2020-05-15
REVISION DATE	2020-05-15

DOCUMENT APPROVAL

NAME	ROLE	DATE
AUTHOR:		
Sipho Ngobeni	Cybersecurity Specialist, CSIR	2020-01-23
REVIEWER(S):		
Noma-Efese Mnqeta	Deputy Director: Cybersecurity Operations, DCDT	2020-02-24
Christo Coetzer	Research Group Leader, CSIR	2020-04-11
Siphokazi Nyangiwe	Director: Cybersecurity Operations, DCTD	2020-05-13
APPROVER(S):		
Kiru Pillay	Chief Director: Cybersecurity Operations, DCDT	2020-05-15

REVISION HISTORY

VERSION NO	AUTHOR	DATE	DESCRIPTION
1.0	Sipho Ngobeni	2020-01-23	Initial version with document structure
1.1	Noma-Efese Mnqeta	2020-02-24	Major review
1.2	Christo Coetzer	2020-04-11	Major review
1.3	Siphokazi Novukuza	2020-05-13	Major review
1.4	Kiru Pillay	2020-05-15	Document review and approval

CSIR, Meiring Naude Road, Brummeria, Pretoria, 0001, South Africa; cshubcsirt@cybersecurityhub.gov.za

2 CONTACT INFORMATION

2.1 Name of the Team

CSHUB-CSIRT

Cybersecurity Hub-Computer Security Incident Response Team.

2.2 Address

CSIR, Meiring Naude Road, Brummeria, Pretoria, 0001, South Africa.

2.3 Time Zone

UTC +02

2.4 Telephone Number

N/A

2.5 Facsimile Number

N/A

2.6 Other Telecommunication

General information about CSHUB-CSIRT can be found at: https://www.cybersecurityhub.gov.za.

2.7 Electronic Mail Address

cshubcsirt@cybersecurityhub.gov.za

2.8 Public Key and Other Encryption Information

CSHUB-CSIRT <cshubcsirt@cybersecurityhub.gov.za>
4096R/F6C12ADD 2020-06-26
Fingerprint= BE6A 6790 595F 18D3 B643 F597 1994 A82B F6C1 2ADD

2.9 Team Members

Team members of the CSHUB-CSIRT are employees of the Department of Communications and Digital Technologies (DCDT).

2.10 Other Information

All contact information about the CSHUB-CSIRT can be found in the webpage:
https://www.cybersecurityhub.gov.za/contact-us/contact-details

2.11 Points of Constituent Contact

Preferred method for contacting CSHUB-CSIRT is via email at cshubcsirt@cybersecurityhub.gov.za, or by reporting an incident via the website: https://www.cybersecurityhub.gov.za.

3 CHARTER

3.1 Mission Statement

The mission of the CSHUB-CSIRT is to be a central point of collaboration of cybersecurity incidents for the private sector, civil society and citizens including incident coordination, information dissemination, awareness building, sector CSIRTs establishment, creation and the promotion of national standards.

3.2 Supporting Objectives

The following objectives allows the CSHUB-CSIRT to serve the South African private sector and civil society in order to execute its mission:

- Coordinate general Cybersecurity activities, in consultation with the Cybersecurity Response Committee (CRC) under the Justice, Crime Prevention and Security (JCPS) cluster of departments within the South African government;
- Identifying stakeholders and establishing public-private relationships whilst collaborating with existing private sector CSIRTs;
- Disseminate relevant information to other sector CSIRTs, vendors and technology experts on Cybersecurity developments;
- Provide best practice guidance on ICT security for business and civil society;
- Initiate Cybersecurity awareness campaigns; and
- Promote compliance with standards, procedures and policies developed by the CRC regarding Cybersecurity matters with a bearing on national security.

3.3 Constituency

The CSHUB-CSIRT constituents are private sector[1], civil society and citizens of the Republic of South Africa

Constituency Type = Mixed

3.4 Sponsorship and/or Affiliation

All activities of the CSHUB-CSIRT are funded by DCDT.

3.5 Authority

CSHUB-CIRT operates under supervision of the Chief Director: Cybersecurity Operations, DCDT.

4 POLICIES

4.1 Types of Incident and Level of Support

The CSHUB-CSIRT is authorised to coordinate cybersecurity incidents such as abusive content, copyright act violation, criminal activity, data breach, denial of service, email attack, identity data exposure, malicious code / malware activity, phishing, physical security, policy violation, reconnaissance activity, unauthorised access and unpatched vulnerability for its constituents. In some instances, the level of support is specified in the memorandum of understanding (MOU) between CSHUB-CSIRT and the respective constituent.

[1] For the purposes of the CSHUB-CSIRT, the private sector refers to organisations not under control of the State.

CSIR, Meiring Naude Road, Brummeria, Pretoria, 0001, South Africa; cshubcsirt@cybersecurityhub.gov.za

4.2 Cooperation, Interaction and Disclosure of Information

All incoming information is tagged as either a Confidential or Public. To support Traffic Light Protocol (TLP) scheme all incoming information marked as TLP:RED, TLP:AMBER or TLP:GREEN is considered as a Confidential internally. TLP:WHITE marking is tagged as a Public accordingly.

Confidential information can be distributed internally on need-to-know basis according to the business needs and cannot be disclosed to third party persons who are not explicitly authorised to receive the information. It is the responsibility of the employee to take necessary measures in order to avoid unauthorised disclosure of Confidential information. Confidential information can be disclosed to the third parties through approval by the associated service owner and then by CSHUB-CSIRT team leader (if differs).

Public information can be released freely after applying appropriate information generalisation and anonymisation techniques.

Incident information can be disclosed according to the stipulations in the MOU with constituents. All incoming incident related data is considered as Confidential and is handled accordingly.

4.3 Communication and Authentication

PGP is considered as a preferable and secure method to protect information. CSHUB-CSIRT has a team key as described in Section 2.8. Every team member possess personal PGP key in order exchange personal messages in secure manner.

5 SERVICES

5.1 Reactive Services

- Incident coordination

5.2 Proactive Services

- Cybersecurity assessments and advisory services
- Announcements
- Security-related information dissemination

5.3 Security Quality Management Services

- Cybersecurity awareness building
- Identification of national standards
- Promotion of national standards
- Establishment of sector-CSIRTs
- Skills and training

6 INCIDENT REPORTING

Cybersecurity incidents can be reported either by sending an email to cshubcsirt@cybersecurityhub.gov.za, or by clicking on the “REPORT INCIDENT” tab on the home page of the CSHUB-CSIRT website: https://www.cybersecurityhub.gov.za.