SANReN CSIRT Charter

RFC2350

Contents

ABBREVIATIONS 3
DOCUMENT INFORMATION 4
CONTACT INFORMATION 6
1. Name of the Team 6
2. Address 6
3. Time Zone 6
4. Telephone Number 6
5. Facsimile Number 6
6. Other Telecommunication Methods 6
7. Electronic Mail Address 7
8. Public Keys and Encryption Information 7
9. Team Members 7
10. Other Information 7
11. Points of Customer Contact 7
CHARTER 8
1. Mission Statement 8
2. Constituency 8
3. Sponsorship and/or Affiliation 8
4. Authority 9
POLICIES 9
1. Types of Incidents and Level of Support 9
2. Co-operation, Interaction and Disclosure of Information 9
3. Communication and Authentication 10
SERVICES 10
1. Vulnerability Assessments 10
2. Announcements 10
3. Resources 11
4. Incident Response Support and Coordination 11
INCIDENT REPORTING FORM 11
DISCLAIMER 11

ABBREVIATIONS

AUP	Acceptable Usage Policy
CSIR	Council for Scientific and Industrial Research
CSIRT	Cyber Security Incident Response Team
DSI	Department of Science and Innovation
IT	Information Technology
NICIS	National Integrated Cyberinfrastructure System
PGP	Pretty Good Privacy
SA NREN	South African National Research and Education Network
SANReN	South African National Research Network
TENET	Tertiary Education and Research Network of South Africa
TLP	Traffic Light Protocol

DOCUMENT INFORMATION

DOCUMENT TITLE	SANReN CSIRT Charter
DOCUMENT NUMBER	CSIR/NICIS/SANReN/CSIRT/FRAM/2024/0001/A
DOCUMENT VERSION NUMBER	v2.3
EFFECTIVE DATE	2024/05/09
REVISION DATE	2026/01/20

APPROVAL		
NAME	ROLE	DATE
AUTHOR:		
Dr Heloise Meyer	Senior SANReN Engineer and Network Security Specialist	2026/01/20
REVIEWER(S):		
Mr Anele Siwela	Junior Cybersecurity Specialist	2026/01/20
Ms Zoya Vilakazi	Junior Cybersecurity Specialist	2026/01/20
APPROVER:		
Mr Sabelo Dlamini	SANReN Director	

REVISION HISTORY			
VERSION NO	**AUTHOR**	**DATE**	**DESCRIPTION**
2.0	Heloise Meyer	2024/05/09	Major Review
2.1	Heloise Meyer	2025/02/24	Minor Review
2.2	Heloise Meyer	2025/08/01	Minor Review
2.3	Heloise Meyer	2026/01/20	Minor Review

CONTACT INFORMATION

1. Name of the Team

SANReN CSIRT
South African National Research Network (SANReN) Computer Security Incident Response Team (CSIRT)

2. Address

SANReN CSIRT
CSIR
Building 43
1 Meiring Naudé Road
Brummeria
Pretoria, 0081
South Africa

3. Time Zone

SAST (UTC+0200)

4. Telephone Number

+27 12 8427 six-five-eight – Dr Heloise Meyer (business hours only).

5. Facsimile Number

Not available. Please call/email upfront if required.

6. Other Telecommunication Methods

Not available.

7. Electronic Mail Address

csirt{at}sanren.ac.za – relays to all SANReN CSIRT members.

The use of our PGP key is advised to encrypt sensitive information.

8. Public Keys and Encryption Information

The SANReN CSIRT team's PGP key can be found on the following public key server - https://pgp.circl.lu/

KeyID	0xA7081DB67F352F2A
Fingerprint	0A9F E785 1857 50AD 05CA A188 A708 1DB6 7F35 2F2A

Individual team members' keys are available on request.

9. Team Members

Operations Manager: Dr Heloise Meyer

Junior Cybersecurity Specialist: Mr Anele Siwela

Junior Cybersecurity Specialist: Ms Zoya Vilakazi

10. Other Information

All contact information about the SANReN CSIRT can be found on the website: https://csirt.sanren.ac.za/

11. Points of Customer Contact

The preferred method for contacting the CSIRT is via e-mail "csirt{at}sanren.ac.za". Please place your institution's name in the subject line.

The SANReN CSIRT team is typically available from 09:00-16:00 SAST Monday to Friday, except for public holidays and 25 December to 1 January. We do not provide a 24x7 service.

Should it not be possible (or advisable for security reasons) to use e-mail, the SANReN CSIRT can be reached by telephone (see 4. Telephone Number) during regular office hours (minimally 9 am to 4 pm SAST). Voice messages are reviewed.

Alternatively, the Tertiary Education and Research Network of South Africa (TENET) can be contacted for reactive (e.g. incident response) services via email "csirt{at}tenet.ac.za".

CHARTER

1. Mission Statement

The mission of the SANReN CSIRT is to provide proactive Information Technology (IT) security services to the sites and users of the SANReN network; to minimise the occurrence of incidents and to equip the constituency to better safeguard against malicious activity.

2. Constituency

The constituency describes the beneficiaries of the SANReN network, including customers of TENET, defined as the "campuses of South African education and research institutions and associated support institutions in the public sector that connect to the network". More formally, the constituency can be defined as

.ac.za domain registrants and/or

users of systems and IP addresses in AS 2018 (TENET's autonomous system)

as clarified by the TENET connection policy.

3. Sponsorship and/or Affiliation

The SANReN CSIRT is primarily funded via the Department of Science, Technology and Innovation (DSTI) of South Africa as part of the SANReN project. The SANReN team (including the CSIRT) is hosted by the Council for Scientific and Industrial Research (CSIR) Next Generation Enterprises and Institutions (NGEI) Cluster and is a key component of the National Cyberinfrastructure System (NICIS), alongside the Center for High Performance Computing (CHPC) and the Data Intensive Research Initiative of South Africa (DIRISA).

The CSIRT services are offered in partnership with TENET, which operates the South African National Research and Education Network (SA NREN), to prevent and respond to IT security incidents. For further relationship details, please see the SANReN website: https://www.sanren.ac.za/

Some services (e.g., vulnerability assessments) are charged for on a cost recovery basis.

4. Authority

The primary objective of the SANReN CSIRT is to proactively mitigate IT security-related issues affecting the SA NREN and constituency, as described in the Services section. This is achieved in an advisory role. Accordingly, the team has limited/indirect authority over the constituency.

The TENET AUP defines acceptable use of the SA NREN, and infringements could result in intervention by TENET.

POLICIES

1. Types of Incidents and Level of Support

The SANReN CSIRT does not directly handle incidents. The constituency is, however, welcome to contact the team for IT security-related advice at any time (including during an incident). The response will be on a best-effort basis, depending on the current load and availability of CSIRT members.

2. Co-operation, Interaction and Disclosure of Information

The SANReN CSIRT follows the principle of responsible disclosure within the bounds of policy and legislation. The information security traffic light protocol is used to classify information handled by the CSIRT as follows:

TLP:RED - Not for disclosure, restricted to participants only (most sensitive).
TLP:AMBER - Limited disclosure, restricted to participants and organisations on a need-to-know basis (sensitive).
TLP:AMBER+STRICT restricts sharing to the organisation only.
TLP:GREEN - Limited disclosure, restricted to the community and related organisations (less sensitive).
TLP:CLEAR - Unrestricted disclosure, public (not sensitive).

For the SANReN CSIRT:

- Participants = the CSIRT team member(s) involved in the exchange only.
- Organisations = SANReN + TENET.
- Community = constituency.

A constituent may request that information be handled at a preferred level; otherwise, the CSIRT will classify it at a level it deems appropriate. Where practicable, the SANReN CSIRT will seek authorisation from a constituent before sharing sensitive information, which will also be anonymised if it does not affect the value/use of the information (e.g. redaction of site identifiable information).

3. Communication and Authentication

Given the types of information that the SANReN CSIRT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP should be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission. Please contact the CSIRT before sending sensitive information if assistance is required (for example, in setting up PGP or an alternative secure mechanism).

SERVICES

The SANReN CSIRT offers the following services as per our website. These services are only available to the constituency (exceptions on agreement).

1. Vulnerability Assessments

The SANReN CSIRT offers a vulnerability scanning service to constituents. This is a process to identify, classify, report on and provide remediation advice on the security weaknesses of specific IT infrastructure. The service helps institutions identify and remedy vulnerabilities to prevent an attack/compromise. Both external and internal scans can be performed.

2. Announcements

The SANReN CSIRT provides an "announcements" service to highlight recent cybersecurity news, including alerts/warnings (e.g. intrusions, threats), advisories (e.g. vulnerabilities, bulletins), articles (e.g.

interesting news) and any other security-related information (e.g. team updates) that may be of interest to the constituency.

Mechanisms for disseminating these announcements include the SANReN CSIRT website and announcement mailing list. Subscription requests to join the announcements mail list can be sent to "csirt-news+subscribe@sanren.ac.za". The mailing list is only available to constituency representatives.

3. Resources

The SANReN CSIRT provides a "resources" service that offers a collection of cybersecurity incident response playbooks providing a consistent approach to follow when remediating a cybersecurity incident. Cybersecurity awareness material is also made available to the beneficiaries of SA NREN.

4. Incident Response Support and Coordination

The SANReN CSIRT offers incident response support and coordination to constituents affected by IT security incidents. The support offered by the SANReN CSIRT will be on a best-effort basis, depending on the type of incident, as well as the availability of CSIRT members. Should the CSIRT deem it necessary, affected constituents will be referred to external providers for specialised cybersecurity services.

INCIDENT REPORTING FORM

Not applicable.

DISCLAIMER

This information is accurate at the publication date.

While every precaution will be taken in the preparation of the website, information, notifications, and alerts, the SANReN CSIRT (and sponsors/affiliates) assume no responsibility for errors or omissions, or damages resulting from the use of the information contained therein, including this document.