



NAMIBIA CYBER SECURITY INCIDENT RESPONSE TEAM

RFC 2350

Contents

- 1. DOCUMENT INFORMATION 3
 - 1.3 Locations where this Document May Be Found 3
 - 1.4 Authenticating this Document..... 3
 - 1.5 Document Identification 3
- 2. CONTACT INFORMATION..... 3
 - 2.1 Name of the Team 3
 - 2.2 Address 4
 - 2.5 Electronic Mail Address 4
 - 2.6 Public Keys and Encryption Information..... 4
- 3. CHARTER 5
 - 3.1 Mission Statement 5
 - 3.2 Constituency 5
 - 3.3 Sponsorship and/or Affiliation 5
 - The NAM-CSIRT is housed under the ambit of the Communications Regulatory Authority of Namibia..... 6
 - 3.4 Authority..... 6
- 4. POLICIES 6
 - 4.1 Types of Incidents and Level of Support 6
 - 4.2 Co-operation, Interaction and Disclosure of Information..... 6
 - 4.3 Communications and Authentication..... 6
- 5. SERVICES 7
 - 5.1 Proactive services 7
 - 5.2 Re-Active Services 7
- 6. Incident Reporting 7
- 7. Disclaimer..... 8

1. DOCUMENT INFORMATION

This document contains a description of the Namibia Cyber Security Incident Response Team (herein after referred to as "NAM-CSIRT") in accordance with RFC 2350¹. It outlines expectations for computer security incident response and guidance on the work of the NAM-CSIRT.

1.1 Date of Last Update

Version 1.1 – 1 April 2025

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:

<https://nam-csirt.na/about/>

1.4 Authenticating this Document

This document has been signed with the PGP public key of NAM-CSIRT. See section 2.6 below for more details.

1.5 Document Identification

Title	RFC 2350 NAM-CSIRT
Version	1.1
Document Date	1 April 2025
Expiration	This document is valid until superseded by a later version.

2. CONTACT INFORMATION

2.1 Name of the Team

Full Name	Namibia Cyber Security Incident Response Team
Short name	NAM-CSIRT

¹ <http://www.ietf.org/rfc/rfc2350.txt>

2.2 Address

Courtside Building (3rd & 4th Floor) Freedom Plaza
c/o Fidel Castro & Rev. Michael Scott Street
Private Bag 1330, Windhoek
Namibia

2.3 Time Zone

Central Africa Time zone: UTC+2

2.4 Telephone number

T: +264 61 222 666

2.5 Electronic Mail Address

For information and operational matters, please email to info@nam-csirt.na and for incident reporting and alerts email to report@nam-csirt.na. The email addresses are monitored by duty officers during hours of operations.

2.5 Other Telecommunication

None

2.6 Public Keys and Encryption Information

Please use the following key during functional exchanges (incident reports, alerts, etc.) with us. Fingerprint	F04A1C8FACAD8B860D5EA2678351BB7089B90123
Location for the PGP Key	nam-csirt.na/PUBLIC-KEY.txt

2.7 Team Members

The head of NAM-CSIRT is Emilia Nghikembua. Information about other team members is available on request. The team has 4 team members.

General information about NAM-CSIRT is available at <https://nam-csirt.na>

- NAM-CSIRT is a member of Global Forum on Cyber Expertise (GFCE)
- NAM-CSIRT complies with the CSIRT Code of Practice³
- NAM-CSIRT supports the use of the Information Sharing Traffic Light Protocol

Days of Operation

Our days of operation are from 08:00 to 17:00 GMT+2 on business days Monday to Friday. We may operate out of these hours and days in case of emergency only.

Emergency Cases: If it's not possible to use e-mail, please call mobile numbers +264811652860 and +264811482907.

3. CHARTER

3.1 Mission Statement

NAM-CSIRT's mission is to pioneer Namibia's cyber defence, ensuring digital security and infrastructure resilience.

Our key values include:

- To ensure that we take the lead in protecting Namibia from cyber threats by implementing strong security measures.
- To help in ensuring that all digital data, from personal information to government records, is kept safe and secure from potential cyber-attacks.
- To build a robust and resilient digital infrastructure that can withstand cyber threats, ensuring that Namibia's digital services remain available and reliable.

3.2 Constituency

The constituency of NAM-CSIRT is composed of all critical infrastructure and critical information infrastructure institutions, bodies, and agencies within the Republic of Namibia.

3.3 Sponsorship and/or Affiliation

The NAM-CSIRT was established in accordance with a policy decision taken on 23rd of November 2023 by the Government of the Republic of Namibia.

The NAM-CSIRT is housed under the ambit of the Communications Regulatory Authority of Namibia.

3.4 Authority

The team coordinates cybersecurity incidents on behalf of its constituency and has no authority to achieve further than that. The team is, however, expected to make operational, non-obligatory recommendations in the course of their work. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made

4. POLICIES

4.1 Types of Incidents and Level of Support

All cyber security incidents are considered a normal priority unless they are explicitly labelled **URGENT** or an **EMERGENCY**. The NAM-CSIRT is committed to keep its constituents informed of potential vulnerabilities and existing threats before they are actively exploited. Special attention will be given to issues affecting critical infrastructure, and critical information infrastructure.

4.2 Co-operation, Interaction and Disclosure of Information

NAM-CSIRT regards the importance of operational co-operation and information sharing between CIRTs, CERTs and other organisations which may contribute towards or make use of their services with the utmost importance. NAM-CSIRT cooperates with other organizations like the law enforcement agencies to protect the privacy of its constituency and stakeholders and operates within the laws of Namibia when disclosing information.

4.3 Communications and Authentication

NAM-CSIRT protects sensitive information in accordance with the relevant legislation, regulations, and policies within the Republic of Namibia. NAM-CSIRT respects the sensitivity marking allocated by originators of information communications to NAM-CSIRT ("originator control").

Communications security (encryption and authentication) is achieved by various means. PGP or other agreed means, depending on the sensitivity level and contest.

5. SERVICES

5.1 Proactive services

- **Announcements** including amongst other things, security advisories, intrusion alerts and vulnerability warnings to inform constituents on issues with a medium to long term impact enabling them to protect their systems and networks before it can be exploited.
- **Technology Watch** assessing new technical developments, intruder activities and trends to extract information relevant to the security of the constituent's systems and networks. It may further include liaison with other authorities to ensure that the most accurate information is obtained before making announcements, providing guidelines and/or recommendations focused on medium to long term security issues.

5.2 Re-Active Services

Alerts and warnings through dissemination of information to constituents pertaining to:

- Intruder attacks;
- Security vulnerabilities;
- Intrusion alerts;
- Computer viruses, hoaxes, etc.;
- And provide a short, recommended course of action to provide guidance for recovering any affected systems or protecting their systems.

6. Incident Reporting

Incidents should be reported to NAM-CSIRT by e-mail using the address report@nam-csirt.na preferably encrypted with NAM-CSIRT-Namibia's public key.

In case of an emergency or crisis, please provide NAM-CSIRT with at least the following information:

- Contact details and organizational information – name of person or organization name and address, e-mail address, telephone number;
- Short summary of the incident/emergency/crisis, type of event;
- Source of indication (e.g., the system produced an alert, etc.);
- System affected;
- The event/incident (e.g., which system produced the alert);
- Estimated impact; and
- Other particulars.

7. Disclaimer

Whilst every precaution will be taken in preparation of information, notification and alerts, NAM-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.

Digitally signed by:

Mrs. Emilia Nghikembua

Head – NAM-CSIRT

Hosted @Communication Regulatory Authority of Namibia

Tel: +264 61 222 666 Email: info@nam-csirt.na

_____ END _____