RFC 2350

Version 2.0 - 09 April, 2025

TLP:CLEAR

Nigeria Computer Emergency Response Team (ngCERT)
No 26 Addis Ababa Crescent,
Wuse Zone 4
Abuja

TABLE OF CONTENTS

Contents

1 Document Information

This document contains a description of ngCERT in accordance with RFC 2350[1]. It provides basic information about ngCERT, its channels of communication, and its roles and responsibilities.

1.1 Date of last update

This is version 2.0 of 09 April 2025.

1.2 Distribution list for notifications

ngCERT does not use any distribution lists to notify about changes in this document. This document is kept up to-date at the location specified in section 1.3.

1.3 Location where this document may be found

The most recent version of this document is available online at the following URL: https://cert.gov.ng/about-us/rfc2350

1.4 Authenticating this document

This document has been digitally signed with the PGP key of Bello Hayatudeen, The Director, Nigeria Computer Emergency Response Team (ngCERT).

1.5 Document Identification

Title: *ngCERT_RFC2350*

Version: *2.0*

Document Date: *09 April, 2025*

Expiration: *This document is valid until superseded by a later version*

2 Contact Information

2.1 Name of the Team

Full name*:* *Nigeria Computer Emergency Response Team*
Short name*:* *ngCERT*

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

2.2 Address

Nigeria Computer Emergency Response Team (ngCERT)
No 26 Addis-Ababa Crescent,
Wuse Zone 4, Abuja
Nigeria

2.3 Time Zone

GMT + 1

2.4 Telephone Number

+234 905 555 4499

2.5 Other Telecommunication

***Twitter**:* *ngCERTofficial*
***LinkedIn**:* *Nigeria Emergency Response Team (ngCERT)*
***Instagram**:* *ngcertofficial*
Facebook: *Nigeria computer Emergency Response Team*

These social media channels are for updates and information and are not monitored for incident reporting. For reporting incidents, please use the designated contact methods provided in section 6.

2.6 Electronic Email Address

For incident reporting, please contact us at:

incident@cert.gov.ng

This email is available and monitored 24/7 by a duty officer.

For operational and non-operational general enquiries, please send us an email at:

info@cert.gov.ng

This is monitored by administrative officer of ngCERT during office hours.

2.7 Public Keys and Encryption Information

We use PGP encryption for secure communication. Please encrypt any sensitive emails using our public key.

Below are our public emails and our corresponding fingerprint keys:

incident@cert.gov.ng

***Fingerprint**:*
5E94 9D2C 84B8 DE99 15D8 938E 6BF6 3323 AF08 A483

***Location**:*
https://cert.gov.ng/contact-us/3323-af08-a483.asc

info@cert.gov.ng

***Fingerprint**: C085 227A BEB3 E9D4 F236 59D1 FB57 8336 F8E6 7B79*

***Location**:*
https://cert.gov.ng/contact-us/8336-f8e6-7b79.asc

2.8 Team Members

ngCERT's team members is not publicly available, Information about the team members might be provided upon request.

2.9 Other Information

See our website https://cert.gov.ng for additional information about ngCERT

2.10 Points of Customer Contact

The preferred method of contacting ngCERT is via email. Please use the official email addresses listed in section 2.6.

Should email not be an option, ngCERT can be reached by telephone. See Section 2.4 for official telephone numbers.

3 Charter

3.1 Mission Statement

The mission of ngCERT as the Nigerian National CERT is

"To achieve a safe, secure and resilient cyberspace in Nigeria that provides opportunities for national prosperity"

3.2 Constituency

The primary constituents of ngCERT encompass all entities utilizing information technology services from the government, public, and private sectors, including

- *All Ministries, Departments and Agencies services;*
- *State Governments;*
- *Critical national infrastructure operators as designated by Nigerian government;*
- *Sectorial CSIRTs and other critical IT infrastructure operators in sensitive sectors.*
- *General Public.*

3.3 Sponsorship and/or Affiliation

ngCERT is a national CERT which operates under the aegis of the National Cybersecurity Coordination Centre (NCCC).

ngCERT is a member of

- *Forum of Incident Response and Security Team*[2]
- *Counter Ransomware Initiatives (CRI)*
- *ECOWAS Information Sharing and Analysis Center (ISAC)*

3.4 Authority

The Nigeria Computer Emergency Response Team (ngCERT) established as National CERT operates under the National Cybersecurity Coordination Centre (NCCC) as mandated by the Cybercrimes (Prohibition, Prevention, ETC) Act 2015.

[2] *https://www.first.org/members/teams/ngcert*

4 Policies

4.1 Types of Incidents and Level of Support

ngCERT is authorized to manage all types of computer security incidents within its constituency, whether they occur or are potential threats. The level of support provided will depend on the incident's type and severity, the constituent involved, the size of the affected user community, and available resources. ngCERT will cooperate promptly and support its constituents, keeping them informed about potential vulnerabilities and assisting in proactive measures to mitigate risks and respond to incidents.

4.2 Co-operation, Interaction, and Disclosure of Information

ngCERT treats all information as confidential by default, but highly regards the importance of operational cooperation and information sharing with other entities in order to fulfil its mission and to help solve security incidents.

ngCERT adheres to the latest Information Sharing Traffic Light Protocol as defined by FIRST[3].Written messages and documents should be clearly tagged with a TLP label. In case of a contact by phone, video conference or similar, the TLP classification should be stated prior to the delivery of the information. By default, ngCERT uses TLP: AMBER+STRICT as defined in TLP version 2.0

It is recommended to encrypt digitally transferred sensitive information, e.g., with the PGP key mentioned in section 2.7.

4.3 Communication and Authentication

To ensure confidentiality and authenticity of information use PGP signatures and encryption (see section2.7) or other agreed upon signing and encryption methods.

5 Services

5.1 Incident Response

ngCERT as the national CERT provide operational assistance to Sectorial CSIRT and her constituents in handling the technical and organizational aspects of incidents. In particular with the following aspect of incident management.

[3] *https://www.first.org/tlp/*

5.1.1 Incident Triage

- *Validating an Incident*
- *Assess and prioritizing the incident*

5.1.2 Incident Coordination

ngCERT as the National CERT plays a crucial role in coordinating cybersecurity incidents by;

- *Ensuring all involved organizations were contacted and determine if any additional contact needs to be made;*
- *Facilitate contact to other parties which can help resolve the incident (in needed) including other National CERTs, Sectoral CERTs, International and local security teams;*
- *If any help is needed, it will facilitate contacting the involved organizations to help them to take the appropriate steps.*
- *Asking for reports and/or composing reports, depending on the involved organizations, incident type and severity.*

5.1.3 Incident Resolution

- *Technical Assistance in remediation and containment depending on severity and affected party as defined in section 4.*
- *Advising the involved organization(s) on appropriate measures.*
- *Following upon the progress of the incident resolution process.*
- *Collecting, analyzing and interpreting evidentiary data, if applicable.*

ngCERT will also collect statistics about incidents within its constituency.

5.2 Proactive Services

- *Raise security awareness in its constituency;*
- *Provide formal training in incident management to sectorial CERT and Constituents;*
- *Technology watch to monitor current trends;*
- *Collect, verify, enrich and redistribute data feeds*
- *Transfer relevant knowledge to the constituency, through best practices documents, presentations and training;*
- *Provide fora for community building and information exchange within the constituency;*
- *Collect contact information of local security teams.*

5.3 Vulnerability Management

- *Discovery and research of vulnerabilities*
- *Management of vulnerability reports*
- *Analysis of vulnerabilities*
- *Support for product vendors in releasing Common Vulnerabilities and Exposures (CVE) reports*
- *Coordinated Vulnerability Disclosure (CVD)*

6 Incident Reporting forms

Incidents should be reported on the ngCERT Incident Reporting Platform, an online platform for reporting cybersecurity incidences.

Platform link: https://cert.gov.ng/incident-report/corporate (for corporate)

https://cert.gov.ng/incident-report/individual (for individual)

Incidents can also be reported by:

Email to the email address incident@cert.gov.ng preferably encrypted with our PGP public key.

In person at the ngCERT office (see Section2.2)

When contacting us, please provide the following information:

- *Contact and Organizational Details: Include the name of the person, organization name and address, email address, and telephone number.*
- *Incident/Event Summary: Provide a brief overview of the incident or event.*
- *Affected Systems: Specify the systems that are impacted.*
- *Assessed Impact: Describe the estimated impact, such as loss of communications.*
- *Additional Information: Include any relevant details that led to the discovery of the incident, such as scanning results or log extracts showing the problem.*

7 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, ngCERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.