

## NITDA-CERRT RFC 2350 DESCRIPTION

### 1. About this document

This document contains a description of NITDA-CERRT in accordance with RFC 2350. It provides basic information about NITDA-CERRT, its channels of communication, and its roles and responsibilities.

#### 1.1 Date of Last Update

This is version 2.0, published on 8<sup>th</sup> September 2025.

#### 1.2 Distribution list For Notification

NITDA-CERRT 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 1.3

#### 1.3 Locations Where this document May Be Found

The current and latest version of this document is available on the NITDA-CERRT website at [cerrt.ng/about-us/NITDA-CERRT-RFC-2350-EN](http://cerrt.ng/about-us/NITDA-CERRT-RFC-2350-EN)

#### 1.4 Authenticating this document

This document has been signed with the PGP key of NITDA-CERRT. The PGP public key, ID and fingerprint are available in section 2.8 of this document.

#### Document Identification

Title: NITDA-CERRT\_RFC2350\_EN

Version: 2.0 Document

Date: 2025-09-08

SHA-256

Expiration: This document is valid until superseded by a later version

### 2. Contact Information

This section describes how to contact NITDA-CERRT

#### 2.1 Name of the Team



CERRT

NITDA-CERRT, National Information Technology Development Agency-  
Computer Emergency Readiness and Response Team

Short Name: NITDA-CERRT

## 2.2 Address

28 Portharcourt Crescent, Off Gimbiya Street, Area 11, Garki, Abuja, Nigeria.

## 2.3 Time Zone

WAT

## 2.4 Telephone Number

+2348178774580

## 2.5 Facsimile Number

N/A

## 2.6 Other Telecommunication

N/A

## 2.7 Electronic Email Address

For General Inquiries: [cerrt@nitda.gov.ng](mailto:cerrt@nitda.gov.ng)

For information Security Incidents: [cerrt.ng/report-incident](http://cerrt.ng/report-incident)

## 2.8 Public Keys and Encryption Information

PGP is used for functional exchanges with NITDA-CERRT

- Key-ID: E717 A31D D773 57FC

- Fingerprint: E63087F9A2760BC3C56D1156E717A31DD77357FC

## 2.9 Team Members

The list of the NITDA-CERRT team members is not publicly available.

Information about the team members might be divulged upon request.

## 2.10 Other information

See our web site at [www.cerrt.ng](http://www.cerrt.ng) for additional information about NITDA-CERRT

### 2.11 Points of Customer Contact

For general inquiries: [cerrt@nitda.gov.ng](mailto:cerrt@nitda.gov.ng)

For information Security Incidents: [cerrt.ng/report-incident/](http://cerrt.ng/report-incident/)

We encourage our customers to use our cryptographic key to ensure integrity and confidentiality.

If it is not possible (or not advisable for security reasons) to use e-mail, NITDA-CERRT can be reached by telephone.

Phone: +2348178774580

NITDA-CERRT hours of operation are 24/7 all year long.

## 3. Charter

### 3.1.1. Mandate

The NITDA Computer Emergency Readiness and Response Team (CERRT) is established to address and manage cybersecurity incidents that may impact the Federal Government, its ministries, departments, and agencies (MDAs), or other stakeholders.

### 3.1.2. Mission

To safeguard Nigeria's digital infrastructure by providing proactive and responsive cybersecurity services, fostering resilience, and enhancing the trust of stakeholders in digital systems and services.

### 3.1.3. Vision

A resilient and secure cyberspace for Nigeria's digital economy, built on trust, innovation and collaboration.

## 3.2. Constituency

The primary constituency is composed of all:

- Ministries, Department and Agencies.
- Private Sector

- Other key players in the ICT sectors.
- All citizens of Nigeria

### 3.3. Sponsorship and /or Affiliation

Federal Republic of Nigeria

Federal Ministry of Communications, Innovation and Digital Economy  
(FMCIDE)

### 3.4. Authority

NITDA-CERRT was established in accordance with the mandate of NITDA and in fulfilment of the requirements of the National Cybersecurity Strategy.

## 4. Policies

### 4.1. Types of Incidents and Level of Support

NITDA-CERRT functions as a government CERT, coordinating and facilitating information sharing, providing mitigation strategies and recommendations for incident response and recovery, cyber space monitoring, researching and analyzing trends and patterns of incident activity for government Ministries, Departments and Agencies (MDAs) with extension to the private sector.

The level of support given by NITDA-CERRT will vary depending on the type and severity of the incident, the type of constituent, and the availability of NITDA-CERRT resources at the time.

### 4.2. Co-operation, Interaction and Disclosure of Information

All information received by NITDA-CERRT related to cyber security incidents is considered confidential and is used only to resolve incidents and prevent further incidents. Information that is sensitive (such as personal data, system configurations) or may be harmful, is processed in a secure environment and encrypted, if they must be transmitted over unsecured environment.

The information submitted to NITDA-CERRT may be distributed to interested parties, such as other CERT teams, our technological partners, administrators of the affected resources, other entities included in the national cyber security system, on a need-to-know basis, for the sole purpose of incident handling (i.e., to the extent necessary to identify and

mitigate the threat). No personally identifying information is exchanged, unless explicitly authorized.

### 4.3. Communication and Authentication

The preferred method of communication is email.

1. For low sensitivity information, unencrypted methods such as emails or phones can be used.
2. All sensitive information shared to NITDA-CERRT should be encrypted with our public PGP key detailed in Section 2.8.

## 5. Services

### 5.1. Incident Response

NITDA-CERRT will provide incident response capabilities 24/7 all year long in the following areas:

#### 5.1.1. Incident triage

- Report assessment: Interpretation of incoming incident reports, prioritizing them, and relating them to ongoing incidents and trends.
- Verification: Help in determining whether an incident has really occurred, and its scope.

#### 5.1.2. Incident Coordination

- Information categorization: Categorization of the incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- Coordination: Notification of other parties involved on a need-to-know basis, as per the information disclosure policy.

#### 5.1.3. Incident Resolution

- Technical Assistance: This may include analysis of compromised systems.
- Eradication: Elimination of the cause of a security incident (the vulnerability exploited), and its effects.

- Recovery: Aid in restoring affected systems and services to their status before the security incident.

## 5.2. Proactive activities

### 5.2.1. Announcements

Announcements include intrusion alerts, vulnerability warnings and security advisories. Such announcements inform citizens and companies in NITDA-CERRT constituency about new developments. Announcements enable receivers to protect their systems and networks against newly found problems before they can be exploited.

### 5.2.2. Technology Watch

NITDA-CERRT monitors and observes new technical developments, intruder activities and related trends to help identify threats.

### 5.2.3. Awareness/Advisories

NITDA-CERRT provides a comprehensive and easy-to-use collection of useful advisory information that aids in sensitizing the public and improving security.

### 5.2.4. Education / Training

This service involves providing cyber security training to build and encourage participation in cyber security among citizens, schools/universities and organizations about computer security issues through seminars, workshops, courses and tutorials.

### 5.2.5. Security Audits and assessments

NITDA-CERRT provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards.

### 5.2.6. Reporting

NITDA-CERRT prepares and publishes periodical reports about its operations and cybersecurity.

## 6. Incident Reporting forms

No specific form is needed to report security incidents via email or phone.

When reporting an incident on the NITDA-CERRT website, some key information (contact, description of the incident, etc.) are mandatory. Please visit [certr.ng/report-incident/](http://certr.ng/report-incident/)

## 7. Disclaimer

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