SS CIRT
South Sudan Computer Incident Response Team

A Safer Digital South Sudan

RFC 2350

DOCUMENT CLASSSIFICATION: TLP: CLEAR

www.cirt.gov.ss

Document Information

This document contains a description of SS-CIRT functions, communication channels and the roles and responsibilities in accordance with RFC2350.

Date of Last Update

17th October 2023

Distribution List for Notifications

There is currently no distribution list for notifications of new versions of this document.

Locations Where This Document May Be Found

The current version of this document can be found at the SS-CIRT Website.

Authenticating This Document

This document has been digitally signed by the SS-CIRT Manager.

Document Identification

TITLE	SS-CIRT RFC 2350
VERSION	V1.0
DOCUMENT VALIDITY	Valid until superseded by a later version

Contact Information

NAME OF THE TEAM	South Sudan National Computer Incident Response Team
SHORT NAME	SS-CIRT

Address

Telecom House, Gumbo Juba-South Sudan.

Time Zone

Central Africa Time (GMT+2)

Telephone Number

+211921447922 / +211981447922

Electronic Mail Address

All inquiries relating to general information or SS-CIRT operations should be sent to info@cirt.gov.ss

All inquiries relating to cyber-incidents should be sent to incidents@cirt.gov.ss

In case of an emergency, please contact SS-CIRT via phone on +211981447922.

The SS-CIRT operates from Monday through Saturday for normal working hours (from 9. 00a.m to 5.00 p.m.) and is alert 24 hours.

Other Telecommunication

For additional information, please visit the SS-CIRT website.

Public Keys and Encryption Information

PUBLIC PGP KEY	
LOCATION	

Team Members

No public information is provided about SS-CIRT Team members.

Other Information

SS-CIRT is currently not a member of any CSIRT Organization.

Charter

Mission Statement

To provide a trusted point of contact that ensures the safety of South Sudan's critical information infrastructure, the people, and organizations by effectively and efficiently monitoring, detecting, and responding to cybersecurity incidents through education, training, awareness, and collaboration.

Constituency

The constituents of SS-CIRT include;

- Critical Infrastructure Service Providers
- Government Agencies
- Business entities
- Organizations
- The General Public

Sponsorship and/or Affiliation

SS-CIRT is multi-agency body established under the National Communication Authority of South Sudan.

Authority

The SS-CIRT operates on a no authority model by coordinating incident management through working together with its constituents however, it is not the mandate of the SS-CIRT to take full responsibility in the incident resolution.

Policies

Types of Incidents and Level of Support

All cyber-related incidents are handled according to Priority and Incident Classification Matrix. Incidents classified as High Priority shall be handled first. SS-CIRT is committed ensuring its constituents are informed of potential vulnerabilities and existing threats before they are actively exploited. Special attention will be given to issues affecting critical infrastructure and designated operators.

Co-operation, Interaction, and Disclosure of Information

SS-CIRT takes seriously the importance of operational cooperation and information sharing between constituents and other CSIRTs as a way of collaboration to quickly resolve incidents. The SS-CIRT works together with the law enforcement agencies to protect the privacy of its stakeholders when disclosing incident information and it operates within the laws of South Sudan.

Communication and Authentication

The SS-CIRT protects sensitive information in accordance with the relevant policies. Access to any information is granted on a need to know basis and PGP encryption is used to ensure secure sharing of information.

Services

The SS-CIRT has adopted the ***FIRST CSIRT Services Framework*** and provides assistance on cyber incident Prevention, Detection, Resolution and Advice to its constituents.

Reactive Services

- Incident detection and resolution
- Incident Response
- Incident triage
- Alerts and warnings
- Cyber threat intelligence
- Information security incident coordination

Proactive Activities

- Information dissemination
- Education and awareness raising
- Training on incident management
- Cooperating with other CSIRTs

Service Level

The SS-CIRT will always strive to respond to incoming incident reports within one business day latest. If you haven't received feedback to an incident report after two business days, we request that you contact us again.

Incident Reporting

One can report an incident to the SS-CIRT through any of the following ways;

- The SS-CIRT website https://cirt.gov.ss
- Email incidents@cirt.gov.ss
- Phone number +211921447922 / +211981447922

When contacting us please provide at least the following details;

- The Incident date and time (including time zone)
- Contact details, organizational information, name of a person, organizational name, and address, email address, telephone number
- Short summary of the incident
- The event/incident (e.g. which system produced the alert)
- Affected systems, Source IPs, ports, and protocols
- And any relevant information relating to the incident

Disclaimers

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

SS CIRT
South Sudan Computer Incident Response Team

A Safer Digital
South Sudan

www.cirt.gov.ss