SS CIRT
South Sudan Computer Incident Response Team

A Safer Digital South Sudan

CYBER INCIDENT REPORTING GUIDE

DOCUMENT CLASSSIFICATION: TLP: WHITE

VERSION 1.0

www.cirt.gov.ss

Introduction

The response by SS-CIRT to a reported incident will depend on several factors, including the incident classification and the capacity of the CIRT team, which encompasses management, legal advisors, and other responsible personnel. This guide outlines the procedures for reporting incidents and defines key cyber-related terms used in communication between the SS-CIRT and those reporting cyber incidents. This guide is applicable to all SS-CIRT constituents.

Objective

The objective of this Guide is to provide a guideline to any person reporting an incident to SS-CIRT.

Scope

This Guide pertains to the SS-CIRT Team and its constituents.

List of Abbreviations

CD	Compact Disc
DDOS	Distributed Denial of Service
DNS	Domain Name System
DOS	Denial of Service
DVD	Digital Versatile Disk
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
MITM	Man in the Middle Attack
S1	Severity Level 1
S2	Severity Level 2
S3	Severity Level 3
SS-CIRT	South Sudan Computer Incident Response Team
TLP	Traffic Light Protocol
USB	Universal Serial Bus

Definitions

Event

An Event is any observable occurrence in a system or network. Events can include normal operational activities, such as a user logging into a system, or atypical occurrences that may indicate potential security issues, such as multiple failed login attempts. Events serve as the basic data points that are analyzed to determine whether they may escalate into incidents requiring further investigation or response by the CIRT.

Cyber Incidents

These are single or a series of undesired, unauthorized or unexpected information security events that compromise the confidentiality, integrity, or availability of information systems. These incidents can have various forms and origins, posing threats to the safety and security of our digital environments.

Information Security Event

Information security event is an occurrence on the system, services or network, indicating a possible breach of the information security policy or violation of the safeguards, or a previously unknown situation that may be relevant to the security.

Critical System

Critical system mean system comprised of applications, data, or other resources that are essential for the survival of an organization. In case a critical system is not operational or its operations have been interrupted, the main operations of the organization are significantly disrupted.

Non-critical System

Non-critical system mean system comprised of applications, data or other resources which, if compromised, have no major impact on the performance of the main operations of the organization.

Guidelines for Incident Reporting

An applicant's incident report should include a description of the incident or event, using the appropriatetaxonomy, and as many of the following information:

- Protection of information submitted (Protection level Highly Confidential, Confidential, public)
- Contact Information (Full name, Email address, Phone number)
- Details of the incident
    - Date and time of detection
    - Time zone
    - Level of impact on the organization (Critical, High, Low, No Impact, or Unknown)
    - Current status (On-going, Incident is under control (localized), Incident has occurredpreviously, and Unknown)
    - Number of affected systems (estimate)
    - Features (description) of the incident

- System details
    - Name and address (Host / IP)
    - System function (e.g. DNS system, Web server, E-mail server, etc.)

Depending on the incident criticality, it is not always possible to gather all the necessary information before reporting the incident. In this case, the person reporting an incident should submit the incident report and continue with additional submissions of information as soon as such information become available.

The Incident Report Form is available on our website(https://cirt.gov.ss/). The fully filled form should be sent to the email; incidents@cirt.gov.ss

All other inquiries relating to general information or SS-CIRT operations and not pertaining to incidents should be sent to info@cirt.gov.ss

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. Upon submitting an incident report, an acknowledgment email will be sent confirming receipt of the incident report.

After creating the incident report in the SS-CIRT incident tracking system, SS-CIRT team shall commence the incident identification stage (categorizing the incident and assigning its priority). This stage is followed by the incident response stage, which is an integral part of the incident resolution.

The reporting party shall then be informedwhen the incidentis resolved or if any other information or clarification is required.

What Should Not Be Reported to SS-CIRT?

Forgotten Passwords:

Password-related issues should be resolved through standard procedures of an organization or password recovery instructions provided on the website of your online accounts.

Computer Hardware Problems:

Incidents related to physical device malfunctions.

Network Connection Problems:

Issues concerning connectivity without cybersecurity implications.

Blocked/Locked Accounts:

Situations handled by system administrators for security reasons.

Non-Cybersecurity Issues:

Any problem unrelated to cybersecurity, such as general IT queries.

A Safer Digital South Sudan

www.cirt.gov.ss