SL-CSIRT
RFC 2350
DOCUMENTATION

Table of Contents

1. Document Overview

About this document

This document describes SL-CSIRT guidelines in accordance with RFC 2350. It provides basic information about SL-CSIRT, its channels of communication, and its roles and responsibilities.

1.1 Date of Last Update

This is the most recent version as of March 25th, 2025.

1.2 Distribution List for Notifications

SL-CSIRT will periodically review this document but only make changes when necessary. 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 is available at https://www.nccc.gov.sl

1.4 Authenticating this document

This document's English and French versions have been signed with the SL-CSIRT PGP Key. The PGP Public Key, ID and fingerprint are available in Section 2.8 of this document and at our website at https://www.nccc.gov.sl

2. Contact Information

This section describes how to contact SL-CSIRT

2.1 Name of the Team

Full name: Sierra Leone National Computer Security Incident Response Team
Short name: SL-CSIRT

2.2. Address

The National Cybersecurity Coordination Centre,
43J Byrne Lane, Drive 5, Off Wilkinson Road
Freetown
Sierra Leone

2.3. Time Zone

Greenwich Mean Time (GMT).

2.4. Telephone Number

+23230962027

2.5. Other Telecommunication

Not applicable.

2.6. Electronic Mail Address

Report cybersecurity incidents to reporting@nccc.gov.sl

2.7. Public Keys and Encryption Information

SL-CSIRT has a PGP key with fingerprint: 1124 2D11 53FB 3631 62DD 75D4 8D6C D772 6F2D
82D0

2.8. Team Members

The SL-CSIRT Team is composed of IT Security experts. The list of SL-CSIRT Team members is not publicly available. The identity of SL-CSIRT team members might be divulged on a case-by-case basis according to the need-to-know restrictions.

2.9. Other Information

For additional information about SL-CSIRT, visit https://www.nccc.gov.sl

2.10. Points of Customer Contact
E-mail: reporting@nccc.gov.sl
Phone: +23230962027

Online form: https://www.nccc.gov.sl/cyber-aid/

In case of emergency, please use the **[URGENT]** tag in the subject field of your email

2.11. Days of Operation

We operate on a 24/7 basis, Monday through Sunday

3. Charter

3.1. Mission Statement

Our National CSIRT's mission is to safeguard critical infrastructure, protect digital assets, and ensure national cyber resilience through proactive threat detection, incident response, and collaborative information sharing, fostering a secure and resilient digital ecosystem for all citizens.

3.2. Constituency

Sierra Leone CSIRT's primary constituents are located across Sierra Leone and include:

- Ministries, Departments and Agencies

- Critical National Information Infrastructure Providers

- Secondary constituents and all private sector organisations registered in Sierra Leone can also benefit from limited services from SL-CSIRT.

3.3. Sponsorship and/or Affiliation

SL-CSIRT is part of the National Cybersecurity Coordination Centre, which is the single entity responsible for cybersecurity-related issues and the fight against cybercrime.

SL-CSIRT is affiliated with UAE CSIRT, AfricaCERT, INTERPOL

3.4. Authority

The Sierra Leone Computer Security Incident Response was established by the Cybersecurity and Crime Act, enacted in 2021. It includes auditing and inspecting any Critical National Information Infrastructure at any time to ensure compliance with the provisions of this Act.

The SL-CSIRT operates under the authority of the National Cybersecurity Coordination Centre.

4. Policies

4.1. Types of Incidents and Level of Support.

SL-CSIRT is authorised to address all types of computer security incidents within its constituencies. The level of support will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or service, and the available resources at the time of the incident.

4.2. Cooperation, Interaction, and Disclosure of Information

The SL-CSIRT highly regards operational cooperation and information sharing between the national, regional, and international CSIRT communities.

Incident-related information, such as names and technical details, is not published without the stakeholders' agreement. If not agreed upon, the supplied information will be kept confidential. SL-CSIRT will not provide information to third parties unless required by law.

SL-CSIRT uses the information security traffic light protocol to classify information handled by the CSIRT as follows:

TLP:RED - Not for disclosure, restricted to participants only (most sensitive).

TLP:AMBER - Limited disclosure, restricted to participants' organisations on a need-to-know basis (sensitive). Note that TLP:AMBER+STRICT restricts sharing to the organisation only.

TLP:GREEN Limited disclosure, restricted to the community and related organisations (less sensitive).

TLP:CLEAR - Unrestricted disclosure, public (not sensitive).

Information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately. All incident reports will be tagged as AMBER unless otherwise stated.

Where it is necessary to establish trust, for example, before relying on information given to SL-CSIRT, or before disclosing confidential information, the identity and bona fides of the other party will be ascertained to a reasonable degree of trust.

4.3. Communication and Authentication

The preferred method of communication is email. See section 2.8. In cases involving sensitive information, use of PGP/GnuPG is highly recommended.

5. Services

SL-CSIRT collaborates with multiple partners and stakeholders within the CSIRT community. These involve activities, including alerts and advisories and network monitoring, to detect attacks as much as possible. We provide relevant information on threats, trends, and remedies to our constituency (and/or media, if necessary) to raise security awareness and competence. We also support sectoral CSIRT teams.

Key services provided by SL-CSIRT are as follows:

- Information Security Incident Report Acceptance

- Information Security Incident Analysis

- Mitigation and Recovery

- Information Security Incident Coordination

- Alerts and advisories.

- Vulnerability Discovery/Research
- Threat intelligence analysis and sharing.

6. Incident Reporting Forms

Refer to section 2.10

Disclaimers

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

Appendix

Document Revision History

Revision	Description of Change	Effective Date
1st	Document Review	11-03-2025
2nd	Update to mailing list and language review	25-03-2025

Document created by: Dorian Collier & Richmond Redwood-Sawyerr

Reviewed by: Mariama Yormah

SL-CSIRT RFC 2350   TLP: CLEAR