TLP: Clear

Ls ComCSIRT
RFC 2350

LESOTHO
COMMUNICATIONS
AUTHORITY

TLP: Clear

1 Document Identification

Title:	RFC2350
Version:	1.0
Document Date:	April 1, 2025
Expiration:	This document is valid until superseded by a later version

2 Contact Information

2.1 Name of the Team

Full Name:	Lesotho Communications Computer Security Incident Response Team
Short name:	Ls ComCSIRT

2.2 Address

Physical Address:	Lesotho Communications Authority Premises 30 Princess Margaret Road Old Europa Maseru Lesotho
Postal Address:	P.O. Box 15896 Maseru 100 Lesotho

2.3 Time Zone

Time Zone:	Greenwich Mean Time (GMT+2), in Central Africa Time Zone (CAT)

2.4 Telephone Numbers

Telephone Numbers:	+266 2231 3820

2.5 Electronic e-Mail Address

Email Contacts:	For notifications and operational matters info@comcsirt.ls For incident reporting incident@comcsirt.ls

NB: The email address is monitored by officers during operations hours.

2.6 Other Telecommunications

For further information please visit our website at: https://comcsirt.ls

2.7 Public Keys and Encryption Information

Please use the key shown below to encrypt messages that you send to Ls ComCSIRT.

Encryption Key	PGP Key
PGP Key Fingerprint	143F0A432477DF4220FF621CEC996E695DA143AF
Location	https://comcsirt.ls/contact-us/

2.8 Team Members

Team Members:	No public information is available about the Team members

2.9 Other Information

Website:	https://comcsirt.ls
Code of Conduct :	Ls ComCSIRT complies with the CSIRT Code of Practice
Information Sharing:	Ls ComCSIRT supports the use of the Information Sharing Traffic Light Protocol (TLP)

2.10 Days of Operation

Operation Times	08:00 to 17:00 (GMT+2)
Operation Days:	Monday to Friday
Information Sharing:	Ls ComCSIRT supports the use of the Information Sharing Traffic Light Protocol (TLP)
Emergency Cases:	If it's not possible to use e-mail, please call the hotline number +266-22213820

We may operate out of these hours and days in case of emergency only.

3 Charter

3.1 Mission Statement

The mission of the Ls ComCSIRT is to enhance the cybersecurity posture of the communications sector by focusing on the detection, prevention, response and recovery. We provide expert advisory services, coordinate incidence response efforts, and promote resilience through continuous education and awareness programs. We aim to create a secure and robust environment that supports the sector's operational continuity and digital growth by fostering collaboration, sharing threats intelligence, and promoting best practices.

3.2 Constituency

The constituency of the Ls ComCSIRT comprises the Communications Service Providers.

3.3 Sponsorship and/or Affiliation

Ls ComCSIRT is a section within the Information & Technology Division of the Lesotho Communications Authority.

3.4 Authority

The Ls ComCSIRT coordinates cybersecurity incidents on behalf of its constituency, without extending its authority beyond this scope. However, the Team is expected to offer operational, best practice, and non-binding recommendations as part of their work. The responsibility for implementing these recommendations rests solely with the recipients, not with the team itself.

4 Policies

4.1 Types of Incidents and Level of Support

All cybersecurity incidents will be given normal priority unless they are explicitly labelled EMERGENCY or URGENT. The Ls ComCSIRT is committed to keep its constituents informed of potential vulnerabilities and existing threats before they are actively exploited.

4.2 Co-operation, Interaction, and Disclosure of Information

Ls ComCSIRT places great importance on operational collaboration and information sharing with other CSIRTs and organisations that benefit from or contribute to its services. The Team will cooperate with entities such as law enforcement agencies to ensure the privacy of our constituents and stakeholders, while strictly adhering to the legal frameworks of Lesotho when disclosing information.

Ls ComCSIRT supports the Information Sharing Traffic Light Protocol (TLP; see https://www.first.org/tlp/docs/tlp-v1.pdf).

Information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

Please visit our privacy statement on https://comcsirt.ls/

4.3 Communication and Authentication

Ls ComCSIRT protects sensitive information in accordance with the relevant policies, and in particular respects the sensitivity markings defined by the originators of information. The Ls ComCSIRT uses the PGP encryption and signing for secure communication.

5 Services

The Ls ComCSIRT has adopted the use of FIRST CSIRT Services Framework and provides assistance on prevention, detection, resolution and advice to its constituents on the following aspects.

5.1 Reactive Services

Reactive services address incidents that have already occurred, focusing on response, coordination, and resolution.

5.1.1 Incident Response

5.1.1.1 Incident Triage

- Validates reported incidents.
- Assesses and prioritizes incidents based on severity and impact.

5.1.1.2 Incident coordination

- Ensures all relevant organisations are contacted and involved.
- Facilitates communication between affected parties and external organisations.
- Acts as an information hub to route incident report effectively

5.1.1.3 Incident resolution

- Advises security teams and system administrators on remediation steps.
- Tracks incidents for situational awareness and reporting purposes.
- Identifies patterns or new types of incidents to guide future preventative efforts.

5.1.2 Cyber Threat Intelligence (CTI)

- Analyses and disseminates threat information to respond to ongoing incidents.
- Integrate CTI into incident triage and resolution measures.

5.2 Proactive Services

Proactive services aim to prevent incidents and strengthen the cybersecurity posture of the constituency.

5.2.1 Education and Awareness

5.2.1.1 Information Dissemination and Campaigns:

- Shares updates on cybersecurity trends, threats, and vulnerabilities.
- Promotes understanding of cybersecurity issues and safe practices.

5.2.2 Collaboration and Knowledge Sharing

5.2.2.1 Cooperation with Other CSIRTs:

- Builds and maintains partnerships with national and international CSIRTs for knowledge sharing and collaboration.

5.2.3 Threat and Vulnerability Management

- Issues advisories on known vulnerabilities and recommended actions.
- Processes and shares actionable insights from data feeds.
- Maintain updated directories of local security teams for effective coordination.

5.3 Service Level

Ls ComCSIRT aims to respond to incident reports within one business day. However, this is dependent on the CSIRT's human capacity, and therefore cannot always be guaranteed.

6 Incident Reporting

Incident reporting shall be sent via an encrypted platform on the following link: https://comcsirt.ls/incident-reporting.

When contacting us via email at incident@comcsirt.ls, please provide the following:

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

7 Disclaimers

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