LESOTHO
COMMUNICATIONS
AUTHORITY

Ls ComCSIRT
Incident Reporting Guidelines

DOCUMENT CLASSSIFICATION: TLP: CLEAR
VERSION 1.0

Introduction

This guideline outlines the procedures for constituents of the Ls ComCSIRT (Lesotho Computer Security Incident Response Team) to report cybersecurity incidents. Prompt and accurate reporting is crucial for effective incident response and helps us protect the sector's digital environment. The response by Ls ComCSIRT to a reported incident will depend on factors such as the incident's severity and the capacity of our team.

Objective

The objective of this guide is to provide clear and straightforward instructions for any individual or organization in Lesotho to report a cybersecurity incident to Ls ComCSIRT.

Scope

This guide applies to all constituents of the Ls ComCSIRT who wish to report a cybersecurity incident.

What is a Cybersecurity Incident?

A cybersecurity incident is a single or a series of unwanted or unexpected events that compromise the **confidentiality**, **integrity**, or **availability** of information systems or the information they process, store, or transmit. Examples include (but are not limited to):

- Malware infections (viruses, ransomware, spyware)
- Unauthorised access to systems or data
- Denial-of-service attacks that disrupt services
- Data breaches or leaks
- Phishing or social engineering attacks that lead to compromise
- Website defacements
- Policy violations with security implications

How to Report a Cybersecurity Incident

When reporting an incident, please provide as much of the following information as possible. However, if critical information is unavailable initially, submit the report with the details you have and provide updates as they become available.

Please include:

- **Your Contact Information:**
  - Full Name
  - Email Address
  - Phone Number

- **Details of the Incident:**
  - **Date and Time of Detection:** When was the incident first noticed? Include the time zone.
  - **Description of the Incident:** Clearly describe what happened. Be specific about the actions taken by the attacker (if known), the impact observed, and any error messages received.
  - **Level of Impact:** How has this incident affected you or your organisation? (e.g., Critical, High, Medium, Low, No Impact, Unknown)
  - **Current Status:** What is the current state of the incident? (e.g., Ongoing, Contained, Eradicated, Recovering, Unknown)
  - **Number of Affected Systems (Estimate):** If applicable, how many devices or systems are involved?
  - **Features/Indicators of the Incident:** What specific signs or symptoms have you observed? (e.g., unusual files, system slowdown, suspicious emails, unauthorized logins)

- **Affected System Details (if applicable):**
  - Name or Hostname of the affected system(s)
  - IP Address(es) of the affected system(s)
  - Function of the System(s): What is the purpose of the affected system? (e.g., Web server, Email server, Database server, User workstation)

- **Protection Level of Affected Information (if applicable):** How sensitive is the information involved? (e.g., Highly Confidential, Confidential, Public)

Reporting Channels:

Please submit incident reports via the following channel:

- **Email:** incident@comcsirt.ls

What Should NOT Be Reported to Ls ComCSIRT:

Please refrain from reporting the following types of issues through the incident reporting channel, as they are typically handled through other standard procedures:

- **Forgotten Passwords:** Password reset requests should be directed to your local IT support or the relevant service provider's recovery process.

- **General Computer Hardware Problems:** Issues related to malfunctioning physical devices (e.g., broken screen, faulty keyboard).
- **General Network Connection Problems:** Connectivity issues that do not have clear cybersecurity implications (e.g., temporary internet outages not linked to an attack).
- **Blocked or Locked Accounts (without suspicion of compromise):** Account lockouts due to too many failed login attempts or other administrative reasons, unless you suspect unauthorized access attempts.
- **General IT Queries or Support Requests:** Questions or requests unrelated to specific security incidents.

Ls ComCSIRT Service Commitment:

Ls ComCSIRT will strive to acknowledge receipt of your incident report within **one business day**. We will then proceed with the initial assessment and prioritization of the incident. Further communication regarding the progress and resolution of the incident will be provided as necessary.

Your cooperation in providing timely and accurate information is vital in our collective efforts to maintain a secure cyberspace for our sector and Lesotho.

Contact Information:

For general inquiries not related to incident reporting, please contact:

Phone: +266 2231 3820, email: info@comcsirt.ls

A Safer Digital Lesotho Ls ComCSIRT : https://comcsirt.ls