LESOTHO COMMUNICATIONS AUTHORITY

Cybersecurity Regulatory Guidelines

Version 1

Revision history

Version	Date	Notes
1.0	March, 2025	First working document

TABLE OF CONTENTS

1 Definitions

For the purposes of these Guidelines, the following terms shall have the meanings set forth below:

"Asset Management" means the process of identifying, tracking, and managing the hardware, software, and data assets that an organisation owns or operates.

"Backup" means the process of creating copies of data or system configurations to ensure recovery in the event of data loss, corruption, or a cybersecurity incident.

"Business Continuity Plan (BCP)" means a documented strategy outlining procedures to ensure the continuation of critical operations during and after a disruptive event, such as a cyber incident or natural disaster.

"Critical Infrastructure" means physical and virtual assets, systems, and networks vital to the communications sector, the destruction or compromise of which would have a significant impact on the security, economy, or public health of the nation.

"Computer Security Incident Response Team(CSIRT)" means a group of cybersecurity experts responsible for receiving, reviewing, and responding to cybersecurity incidents. Their role includes mitigating the impact of security breaches, coordinating incident responses, and providing guidance to prevent future incidents.

"Cybersecurity" means the practice of protecting systems, networks, and data from digital attacks, damage, or unauthorised access through a combination of technologies, processes, and controls.

"Cybersecurity Governance" means a system of policies, roles, and responsibilities within an organisation that ensures effective cybersecurity decision-making and management, aligned with business objectives.

"Data Encryption" means the process of converting data into a code to prevent unauthorised access, ensuring confidentiality and integrity during storage or transmission.

"Data Loss Prevention (DLP)" means tools or processes designed to detect, prevent, and protect sensitive data from being shared or accessed by unauthorised users.

"Firewall" means a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, acting as a barrier between trusted internal networks and untrusted external ones.

"Incident Response Plan" means a structured approach outlining the steps to take following a cybersecurity incident, including detection, containment, eradication, recovery, and post-incident analysis.

"Intrusion Detection System (IDS)" means a system that monitors network traffic for suspicious activity or violations of security policies and alerts administrators to potential threats.

"ISO/IEC 27001" means an international standard that provides a framework for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) to protect sensitive data and ensure organisational resilience against cybersecurity threats.

"Internet Service Provider (ISP)" means a company that provides customers with access to the internet and other related services such as web hosting or email**.**

"Mobile Network Operator (MNO)": means a provider of wireless communications services that owns or controls the necessary infrastructure to deliver mobile services.

"Multi-Factor Authentication (MFA)" means a security system requiring more than one method of authentication from independent categories of credentials to verify the user's identity for access.

"Network Segmentation" means the practice of dividing a network into smaller, isolated segments to limit the spread of cybersecurity threats and reduce the attack surface.

"NIST Cybersecurity Framework (NIST CSF)" means a set of voluntary guidelines developed by the National Institute of Standards and Technology to manage and mitigate cybersecurity risks through core functions such as Identify, Protect, Detect, Respond, and Recover.

"Physical Security" means measures designed to prevent unauthorised access, damage, or interference with physical assets such as buildings, equipment, and other infrastructure components.

"Risk Management" means the process of identifying, evaluating, and prioritising potential cybersecurity risks and implementing strategies to mitigate or manage them.

"Security Information and Event Management (SIEM)" means a system that collects, analyses, and correlates security data from across the network to detect and respond to cybersecurity threats in real-time.

"Segregation of Duties" means a control principle whereby responsibilities and tasks are divided among different individuals to prevent fraud or errors, ensuring that no single person has complete control over a critical process.

"Threat Intelligence" means information about emerging cybersecurity threats and vulnerabilities, enabling organizations to proactively defend against potential attacks.

"Vulnerability" means a weakness or flaw in a system, process, or software that could be exploited by a threat actor to gain unauthorised access or cause harm.

2 Introduction

The cybersecurity landscape is constantly evolving, making it essential for Mobile Network Operators (MNOs), Infrastructure Network Providers, Internet Service Providers (ISPs), and other players in the Communications Sector in Lesotho to adopt robust cybersecurity measures to protect their infrastructure and customers. These guidelines, grounded in international best practices from the NIST Cybersecurity Framework (NIST CSF) and ISO/IEC 27001, aim to bolster the overall cybersecurity posture of the communications sector in Lesotho, ensuring the protection of both infrastructure and customer data.

3 Objectives

The objectives of these guidelines are to:

1.1. **Enhance Cybersecurity Resilience:** Strengthen the cybersecurity resilience of the communications sector in Lesotho.
1.2. **Ensure Compliance:** Align with international best practices and standards to ensure sector-wide compliance (ISO/IEC 27001, NIST CSF, and industry regulations).
1.3. **Promote Cybersecurity Awareness:** Foster a culture of cybersecurity awareness among employees and customers of sector players.
1.4. **Risk Mitigation:** Reduce cybersecurity risks through continious monitoring, governance, and response strategies
1.5. **Comprehensive Security Approach:** Integrate various dimensions of cybersecurity, including physical security, operations security, threat intelligence, and staff training.
1.6. **Strengthen Governance:** Implement robust governance structures to ensure accountability, oversight, and effective management of cybersecurity strategies.

4 Cybersecurity Guidelines

These Guidelines are organised into several key areas, each addressing critical aspects of cybersecurity.

4.1 Cybersecurity Governance and Risk Management

4.1.1 Establish a Cybersecurity Policy

Licensees shall develop and implement a comprehensive cybersecurity policy that aligns with ISO/IEC 27001 or NIST CSF. This policy should include the organisation's commitment to cybersecurity, outlining roles, responsibilities, and processes for managing cyber risks, and serve as a foundation for all security-related activities.

4.1.2 Risk Management

Licensees shall conduct regular risk assessments (i.e. operational, regulatory, etc) to identify, evaluate and mitigate potential cybersecurity threats and vulnerabilities. These assessments should address both internal and external threats, enabling the organisation to prioritise resources and implement effective counter measures.

4.1.3 Cybersecurity Governance Framework

Licensees shall establish a governance structure to oversee the implementation and maintenance of cybersecurity measures within their organisations. This may include the formation of a cybersecurity Steering Committee or a similar body to guide strategic decisions and ensure alignment with business objectives.

4.1.4 Business Continuity Planning (BCP)

Licensees shall develop and maintain a Business Continuity Plan (BCP) that addresses the resilience of critical infrastructure and services in the event of cyber incidents, natural disasters, or system failures. The BCP should include backup and disaster recovery strategies with regular testing exercises.

4.1.5 Security Roles and Responsibilities

Licensees shall clearly define roles and responsibilities related to cybersecurity within the organisation. They should assign specific duties to individuals or teams to ensure accountability and effective management of cybersecurity efforts.

4.1.6 Segregation of Duties

Licensees shall implement controls to ensure the segregation of duties within critical operations. Individuals with administrative access to sensitive systems should not perform conflicting roles, reducing the risk of insider threats or errors.

4.1.7 Security of Third-Party Dependencies

Licensees shall manage the security risks associated with third-party vendors and service providers. This includes conducting due diligence, establishing security requirements in contracts, and regularly monitoring third-party compliance.

4.2 Incident Management and Threat Intelligence

4.2.1 Incident Response Plan

Licensees shall develop and maintain an incident response plan to quickly detect, respond to, and recover from cybersecurity incidents. The plan should outline the steps to take in the event of a breach, including roles, communication protocols, and

recovery procedures. Licensee shall regularly conduct incident response drills to test the effectiveness of the plan.

4.2.2 Incident Reporting

Licensees shall establish reporting protocols for security incidents, notifying both internal stakeholders and external authorities, such as the sectoral or national CSIRT, promptly and with appropriate details.

4.2.3 Threat Intelligence

Licensees shall establish threat intelligence programs to monitor, detect, and respond to emerging cybersecurity threats. Licencees shall also participate in information-sharing communities such as national CSIRTs or sector-specific groups to stay updated on threat trends.

4.3 Physical Security

4.3.1 Securing Physical Infrastructure

Licensee shall establish physical access to critical communication infrastructure (data centers, server rooms, network operations centers). The infrastructure should be restricted to authorised personnel. Licensees shall implement surveillance, access control, and environmental controls to ensure physical security.

4.3.2 Facility Monitoring

Licensees shall deploy security cameras, alarm systems, and biometric access controls to monitor and control physical access to sensitive areas. Physical security breaches that manifest into cybersecurity incident shall be addressed promptly in line with section 4.2.2.

4.4 Access Control

4.4.1 Access Management

Licensees shall implement strong access control measures to ensure that only authorised personnel have access to critical systems and data. This includes the use of role-based access control (RBAC) and least privilege principles to minimise the risk of unauthorised access.

4.4.2 Authentication

Licensees shall ensure that multi-factor authentication (MFA) is used for accessing sensitive systems and data, especially for privileged accounts (See section 3.7.2 on Asset classification).

4.5 Operational Security

4.5.1 Operational Security Controls

Licensees shall implement security controls such as firewalls, IDS/IPS (Intrusion Detection/Prevention Systems), and endpoint protection across all operational networks and devices. Licensees shall ensure systems are patched and updated regularly to mitigate vulnerabilities.

4.5.2 Network Monitoring

Licensees shall continuously monitor networks and systems for suspicious activities.

4.5.3 Auditing

Licensees shall conduct regular audits and vulnerability assessments to identify and mitigate weaknesses in operational security.

4.5.4 Change Management

Licensees shall implement a formal change management process for any updates to systems or infrastructure. Licensees shall ensure that changes are properly reviewed, tested, and approved before implementation.

4.6 Data Protection

4.6.1 Data Availability

Licensees shall ensure that data availability is maintained through redundant systems and backup solutions, allowing for continued operations in the event of system failure or data loss.

4.6.2 Data Encryption

Licensees shall encrypt sensitive data at rest and in transit to protect the confidentiality and integrity of critical information from unauthorised access.

4.6.3 Data Loss Prevention (DLP)

Licensees shall implement DLP solutions to prevent unathorised transfer and sharing of information to ensure the integrity and confidentiality of data.

4.7 Asset Management

4.7.1 Asset Inventory

Licensees shall maintain an up-to-date inventory of all critical assets, including hardware, software, and data. This inventory should be regularly updated to reflect changes in the Information Technology (IT) environment, ensuring that all assets are accounted for and protected.

4.7.2 Asset Classification

Licensees shall classify their assets based on their criticality and sensitivity to ensure appropriate protection measures are applied. This classification should guide the implementation of security controls, prioritising the protection of the most valuable and sensitive assets.

4.8 Network and Information Systems Security

4.8.1 Firewalls and IDS/IPS Deployment

Licensees shall deploy firewalls and IDS/IPS at key network points to protect systems from unathorised access and detect potential instrusions. These shouls be configured, updated and monitored.

4.8.2 Network Segmentation

Licensees shall segment networks to limit the spread of cybersecurity threats and minimise potential damage. Licensees shall also ensure that backup environment is adequately separated from the production environment.

4.8.3 Backup and Recovery

Licensees shall ensure that regular backups of critical systems and data are performed and stored securely. Licensees shall as well test recovery procedures to ensure systems can be restored in the event of data loss or compromise.

4.9 Continuous Monitoring and Improvement

4.9.1 Security Monitoring

Licensees shall implement continuous monitoring of systems and networks to detect and respond to potential threats in real-time. This includes the use of security information and event management systems and other monitoring tools.

4.10 Audit and Compliance

4.10.1 Regular Internal Security Audits

Licensees shall conduct periodic internal security audits, penetration tests and vulnerability assessments to identify and address security weaknesses. Licensees shall also conduct regular internal security audits to ensure compliance with these guidelines and identify areas of improvement. Audit findings should be documented, and action plans should be created to address any issues found.

4.10.2 Annual External Security Audits

Licensees shall engage a qualified third party to conduct annual external security audits and penetration tests to identify and address security weaknesses. Audit findings should be documented, and action plans should be created to address any issues found.

4.10.3 Compliance Monitoring

Licencess shall continuously monitor compliance with these Guidelines, industry standards and any other relevant regulatory requirements.

4.11 Cybersecurity Awareness and Training

4.11.1 General Organisational Awareness

Licensees shall provide regular cybersecurity awareness training to all personnel of the organisation including employees and board of directors to ensure they understand their role in protecting the organisation. Training should cover topics such as phishing, social engineering and safe computing practices.

4.11.2 Customer Awareness

Licensees shall educate customers on best practices for online safety and how to protect their personal information. Customer awareness initiatives may include informational campaigns, online resources and direct communication.

4.11.3 Technical Staff Training

Licensees shall provide continuous training for cybersecurity technical staff on cybersecurity best practices, emerging threats, and new technologies. Training should focus on critical areas such as threat detection, incident response, and secure system configuration. Licensees shall encourage staff to acquire and maintain certifications in recognised cybersecurity disciplines such as CISSP, CEH, or CISM. Staff expertise must align with evolving industry standards to manage and mitigate cybersecurity risks effectively.

4.11.4 Cybersecurity Roles and Responsibilities

Licensees shall appoint a CISO or equivalent position responsible for developing and overseeing cybersecurity programs and ensuring compliance with these guidelines.

4.11.5 Security Team

Licensees shall form a dedicated security team, tasked with implementing security controls, monitoring systems, and responding to incidents.

5 Implementation

5.1 Phased Implementation

Licensees shall implement the Guidelines in phases, starting with critical infrastructure and expanding to cover all areas. A phased approach allows organisations to prioritise resources and focus on the most critical areas first. Licensees shall develop and submit an implementation plan to the Authority.

5.2 Continuous Improvement

LCA shall update the Guidelines periodically to address emerging threats and incorporate new best practices.

6 Security Measures & Evidence Table

Security Measure	Description	Evidence	Reference
Cybersecurity Governance and Risk Management			
Establish a Cybersecurity Policy	Develop and implement a comprehensive cybersecurity policy.	Documented and approved security policy, including scope, critical assets, and the security objectives.	ISO 27001: 5.2, 6.1.1, NIST CSF 2.0: **GV.PO-1**
Risk management	Conduct regular risk assessments to identify and mitigate risks.	Risk assessment reports, risk register, and mitigation plans, including identified threats, vulnerabilities, and corresponding risk ratings.	ISO 27001: 5.2, 6.1.1, NIST CSF 2.0: **GV.RM-1**
Cybersecurity Governance Framework	Establish a governance structure for cybersecurity.	Organisational chart highlighting cybersecurity roles, meeting minutes from governance committee.	ISO 27001: 6.1.2, 6.1.3, NIST CSF 2.0: **GV.GP-1 to GV.GP-3**
Business Continuity Planning (BCP)	Develop and maintain a BCP to ensure resilience during incidents.	Documented BCP, recovery testing results, backup procedures.	ISO 27001: A.17.1, NIST CSF 2.0: **ID.BE-5**
Security Roles and Responsibilities	Assign and define security roles and responsibilities.	Job descriptions, role-based access control (RBAC) matrix, and documented security responsibilities.	ISO 27001: A.7.2.2, A.6.1.1, NIST CSF 2.0: **GV.PO-1**
Secregation of Duties	Ensure duties are segregated to avoid conflicts of interest.	Role-based access control (RBAC) documentation, logs, and access reviews.	ISO 27001: A.6.1.2, A.12.4.3, NIST CSF 2.0: **PR.AC-5**

Security of Third-Party Dependencies	Assess and manage risks associated with third-party vendors.	Third-party risk assessments, vendor contracts with security clauses, and audit reports from third-party security evaluations.	ISO 27001: A.15.1, NIST CSF 2.0: **ID.SC-1**
Incident Management and Threat Intelligence			
Incident Response Plan	Develop and maintain an incident response plan.	Documented incident response plan, incident response team roster, and records of incident response exercises or simulations.	ISO 27001: A.16.1.5, NIST CSF 2.0: **RS.RP-1**
Incident Reporting	Establish procedures for reporting incidents to authorities.	Incident reporting procedure documents, incident logs, and communications with regulatory bodies or authorities.	ISO 27001: A.16.1.2, NIST CSF 2.0: **RS.CO-2**
Threat Intelligence	Implement threat intelligence to stay informed on emerging threats.	Threat intelligence reports, intelligence feeds, and information-sharing activities.	ISO 27001: A.12.6.1, NIST CSF 2.0: **DE.CM-1**
Physical Security			
Securing Physical Infrastructure	Ensure physical infrastructure security to protect critical assets from unauthorised access.	CCTV footage, visitor logs, access cards, and physical security audit reports.	ISO 27001: A.11.1, NIST CSF 2.0: **PR.AC-3**
Facility Monitoring	Continuously monitor the facilities for suspicious activities.	Security logs, camera surveillance records, and physical security reports.	ISO 27001: A.11.1.4, NIST CSF 2.0: **DE.CM-7**
Access Control			
Access Management	Implement strong access control measures.	Access logs, access review reports, and system configuration files enforcing least privilege.	ISO 27001: A.9.1, NIST CSF 2.0: **PR.AC-1**
Authentication	Use multi-factor authentication for sensitive systems.	MFA implementation plan, logs showing successful MFA logins, and documentation of authentication mechanisms in use.	ISO 27001: A.9.4.2, NIST CSF 2.0: **PR.AC-7**
Operational Security			
Operational Security Controls	Implement operational security controls like firewalls, IDS/IPS.	Network diagrams, firewall and IDS/IPS logs, and evidence of patches/updates.	ISO 27001: A.12.1.1, NIST CSF 2.0: **PR.PT-1**
Network Monitoring and auditing	Continuously monitor networks for suspicious activities.	Network monitoring tools, audit logs, and vulnerability assessment reports.	ISO 27001: A.12.4.1, NIST CSF 2.0: **DE.CM-1**
Change Management	Maintain change control for systems and networks.	Change request logs, approval records, and change impact assessments.	ISO 27001: A.12.1.2, NIST CSF 2.0: **PR.IP-3**
Data Protection			
Data Availability	Ensure data availability through reliable backup and recovery processes.	Backup schedules, recovery time objectives (RTO), disaster recovery test results, and incident reports on downtime.	ISO 27001: A.12.3.1, NIST CSF 2.0: PR.IP-4
Data Encryption	Encrypt sensitive data at rest and in transit.	Encryption key management procedures, and encryption implementation reports.	ISO 27001: A.10.1, NIST CSF 2.0: **PR.DS-1, PR.DS-2**

Data Loss Prevention (DLP)	Implement DLP solutions to protect data integrity and confidentiality.	DLP system logs, and incident reports involving DLP alerts.	ISO 27001: A.13.2.1, NIST CSF 2.0: **PR.DS-5**
Asset Management			
Asset Inventory	Maintain an up-to-date inventory of all critical assets.	Detailed asset inventory database, asset tracking system records, and asset classification documentation.	ISO 27001: A.8.1.1, NIST CSF 2.0: **ID.AM-1**
Asset Classification	Classify assets based on criticality and sensitivity.	Asset classification report, data flow diagrams with sensitivity labels, and asset risk assessment records.	ISO 27001: A.8.2.1, NIST CSF 2.0: **ID.AM-2**
Network and Information Systems Security			
Firewalls and IDS/IPS deployment	Deploy firewalls and IDS to monitor and protect network traffic.	Network architecture diagrams showing firewall placement, IDS/IPS logs, and firewall configuration files.	ISO 27001: A.13.1.1, NIST CSF 2.0: **PR.PT-1**
Network Segmentation	Segment networks to limit the spread of cybersecurity threats.	Network segmentation plan, VLAN configuration records, and audit reports confirming network segmentation effectiveness.	ISO 27001: A.13.1.3, NIST CSF 2.0: **PR.PT-4**
Backup and Recovery	Regular backups and testing of recovery procedures.	Backup schedules, recovery test results, and incident response documentation.	ISO 27001: A.12.3.1, NIST CSF 2.0: **PR.IP-4**
Continuous Monitoring and Improvement			
Security Monitoring	Implement continuous monitoring of systems and networks.	Security monitoring system logs, and real-time monitoring dashboards.	ISO 27001: A.12.4.1, NIST CSF 2.0: **DE.CM-1**
Audits and Compliance			
Regular Security Audits	Conduct regular security audits to identify weaknesses.	Audit reports, vulnerability assessment results, and remediation action plans.	ISO 27001: A.18.2.2, NIST CSF 2.0: **GV.CT-1**
Compliance Monitoring	Continuously monitor compliance with industry standards.	Compliance audit reports, certification records, and monitoring logs.	ISO 27001: A.18.1.4, NIST CSF 2.0: **GV.CT-4**
Cybersecurity Awareness and Training			
General Employee Awareness	Provide regular cybersecurity awareness training to all employees.	Training schedules, training materials, attendance records, and employee feedback on training effectiveness.	ISO 27001: A.7.2.2, NIST CSF 2.0: **PR.AT-1**
Customer Awareness	Educate customers on online safety and protecting personal information.	Customer awareness campaign materials, website content with safety tips, and records of customer outreach initiatives.	ISO 27001: A.7.2.2, NIST CSF: **PR.AT-2**
Employee Training	Provide continuous cybersecurity training to technical staff	Training logs, certification records (e.g., CISSP, CEH), and post-training evaluations.	ISO 27001: A.7.2.2, NIST CSF: **PR.AT-3**