Cybersecurity Regulations

LTA – REG – 0013 – 2026

JANUARY 13, 2026

Table of Content

Part I: Preliminary

1.0 Preamble

1.1 These Regulations have been developed by the Liberia Telecommunications Authority (LTA) pursuant to Part III, Section 11 (1) (q) (w) and 11(2) of the Telecommunications Act 2007.

2.0 Purpose of these Regulations

2.1 The purpose of these regulations is to create a framework for ensuring:

A. The safety of telecommunications networks and users of telecommunications services;
B. The protection of privacy and proper use of Personal Data and Personal Identifiable Information;
C. Confidentiality, integrity and availability (CIA) of data and information systems of Telecommunications Service Providers; and
D. The advancement of national cybersecurity capabilities.

3.0 Scope of Application

3.1 These Regulations shall apply to all Telecommunications Service Providers that own, operate, and/or connect to Telecommunications Networks to facilitate or provide Telecommunications Services in Liberia.

4.0 Short Title

These Regulations may be cited as the **"LTA Cybersecurity Regulations 2026".**

5.0 Objectives

5.1 The objectives of these Regulations are as follow:

A. To establish rules, standards, and guidelines for managing cybersecurity risks across Telecommunications Networks;

B. To ensure that all Telecommunications Service Providers implement data protection mechanisms in line with these Regulations, other LTA's Regulations, Orders, Rules, international conventions and/or protocols, and any applicable national laws;

C. To obligate the Telecommunications Sector to undertake training and capacity-building programs in order to develop cybersecurity expertise across the telecommunications sector; and

D. To require Telecommunications Service Providers to report Cybersecurity Incidents promptly.

6.0 Definition of Key Terms

1. "Annual Gross Revenue" means the total revenue generated by Telecommunications Service Provider within a Fiscal Year, encompassing all retail services like fixed telephone, mobile-cellular, Internet, and data services.

2. "Authentication" means the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3. "Availability" means the property of being accessible and usable upon demand by an authorized entity.

4. "Baseline Configuration" means a set of specifications that define the standard, approved, and documented configuration of a system, network, or device. It serves as a reference point for future builds, releases, and changes, ensuring consistency, security, and optimal functionality.

5. "Baseline Framework" means a fundamental set of guidelines, recommendations, or best practices that provide a foundational structure for a specific area of telecommunications or ICT. It serves as a starting point for implementing, testing, or evaluating specific technologies, services, or systems within that area.

6. "Business Continuity" means the capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruptive incident.

7. "Compliance Order" means a formal directive, issued by the LTA, requiring Telecommunications Service Provider to take specific actions to comply with a law, regulation, order, rule and/or other legal obligations.

8. "Computer Emergency Response Team" (**CERT**) means a group of cybersecurity experts responsible for handling major security incidents.

9. "Critical Information Infrastructure" (**CII**) means interconnected information systems and networks that are essential for the functioning of a nation or society. Their disruption or destruction would have a significant negative impact on national security, the economy, public health, or the safety of citizens.

10. "Critical Infrastructure" means systems, facilities, networks, and assets that are essential for the proper functioning of a society's economy, public health or safety, and national security.

11. "Cybersecurity" means the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the Cyber Environment and organization and user's assets.

12. "Cyber Environment" means the online space where cyber threats, including malicious activities, are conducted. It encompasses networks, devices, and processes connected to the internet that can be targeted by cyber threat actors.

13. "Cybersecurity Incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

14. "Cybersecurity Risk" means the potential for harm to an organization or individual's assets in the Cyber Environment, stemming from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

15. "Cybersecurity Risk Management" means the process of identifying, analyzing, evaluating, and addressing an organization's Cybersecurity Threats.

16. "Cybersecurity Threat" means any action or event that has the potential to harm the confidentiality, integrity, or availability of information and its supporting infrastructure. This includes malicious acts targeting systems, data, or networks, such as viruses, malware, data breaches, and denial-of-service attacks.

17. "Cybersecurity Unit" means, an office or a department within an organization that is responsible for managing and mitigating cyber security risks.

18. "Data Minimization" means collecting and retaining only the minimum amount of Personal Data necessary to achieve a specific purpose.

19. "Data Protection" means the safeguarding of Personal Data, ensuring its confidentiality, integrity, and availability while respecting individuals' rights, through a combination of policy, technology, and educational measures, and includes- aspects like access control, encryption, and Data Minimization.

20. "Digital Asset" means any item that exists only in digital form, holds value, and is uniquely identifiable. This value can be tangible or intangible, and digital assets can be created, stored, and traded electronically. Examples include documents, audio, video, and cryptocurrencies, along with their associated usage rights.

21. "Digital Identity" means a unique representation of an individual, organization, or device in a digital environment, used for authentication, authorization, and access control.

22. "Encryption" means the process of converting information or data into a code to prevent unauthorized access.

23. "Fiscal Year" means a 12-month period used for accounting and reporting purposes, which may not coincide with the calendar year. It is a standard period used by governments, businesses, and organizations to track financial activity and prepare budgets and financial reports.

24. "Identity and Access Management" (IAM) means frameworks, processes, and technologies that manage digital identities and control users' access to critical systems.

25. "Incident Response" means the process of identifying, mitigating, and recovering from Cybersecurity Incidents.

26. Incident Response Plan" (IRP) means a detailed written document outlining an organization's procedures for responding to Cybersecurity Incidents, including data breaches, cyberattacks, and other Cybersecurity Threats. It covers the entire incident lifecycle, from preparation and detection to containment, eradication, and recovery, with a focus on minimizing the impact of incidents.

27. "Information Communications Technology" (ICT) means the diverse set of tools and resources used for handling, transmitting, and exchanging information. It encompasses both hardware and software, including computers, the internet, and communication technologies like telecommunications and broadcasting.

28. "Investigate" means the follow-up action to triage, involving in-depth analysis and documentation of a confirmed incident to understand its scope, impact, and root cause.

29. "ICT systems" means a comprehensive setup that utilizes hardware, software, data, and people to facilitate communication, information sharing, and data processing. It encompasses various technologies like computers, networks, the internet, and other devices used for communication and information exchange.

30. "LTA" means the Liberia Telecommunications Authority.

31. "Multi-Factor Authentication" (MFA) means a security measure that requires more than just a password to verify a user's identity before granting access to an account or system.

32. "Person" means a natural or other legally recognized person or entity, and includes a joint stock company, a limited liability company, a partnership, a sole proprietorship, a joint venture, or other form of entity whether incorporated or unincorporated.

33. "Personal Data" means any information relating to an identified or identifiable natural person, also known as a data subject. This means that the information, either on its own or in combination with other data, can be used to identify an individual, either directly or indirectly.

34. "Personal Identifiable Information" (PII) means any data that can be used to directly or indirectly identify an individual. It encompasses a wide range of information, from basic details like names and addresses to more sensitive data like Social Security numbers and financial account information.

35. "Penetration Testing" (also known as Pen Testing or Ethical Hacking), means a simulated cyberattack on a computer system or network to identify and

assess vulnerabilities. It is a proactive security measure where security experts act as adversaries to uncover weaknesses before malicious actors can exploit them.

36. "Sectoral Resilience" means specific sectors, like the Telecommunications Sector, having the capacity to withstand and recover from adverse events, ensuring essential services continue to function.

37. "Security Events" is any observable occurrence within an organization's ICT infrastructure that could potentially compromise the integrity, confidentiality, or availability of data.

38. "Service Level Agreement" (SLA) means a formal contract that defines the level of service to be provided, sets expectations, and holds the provider accountable.

39. "Telecommunications Network" means any wire, radio, optical or other electromagnetic system for routing, switching or transmitting Telecommunications Services between network termination points;

40. "Telecommunications Sector" means the entire field of information and communication technologies (ICTs), including fixed and mobile telecommunications, and internet services. It involves the development, deployment, and management of networks, technologies, and services that facilitate communication and information sharing.

41. "Telecommunications Service" means any provision of the voice and data transmission; SIM cards and pre-paid accessories; equipment and facilities to customers; or any form of transmission of signs, signals, text, images or other intelligence by means of a Telecommunications Network, but does not include a broadcasting service.

42. "Telecommunications Service Provider" means a person or entity under permit or license by the LTA that provides a telecommunications service to the public or that owns or operates a telecommunications network used to provide telecommunications services to the public;

43. "Triage" means the process of assessing, classifying, and prioritizing security alerts and incidents to identify and address the most critical issues first.

44. "The Act" means the Telecommunications ACT 2007.

Part II: Obligations of Telecommunications Service Providers and LTA

7.0 Telecommunications Service Providers' Obligations

7.1 Establishment of a Cybersecurity Unit

A. All Telecommunications Service Providers shall:

i. Establish and maintain a Cybersecurity Unit within their entities to ensure that primary defense against cyber threats is in Liberia; and

ii. The unit shall undergo mandatory cybersecurity examinations conducted by industry certified auditors validated by the LTA.

B. Pursuant to Section 7.1 (A) (i), all Telecommunications Service Providers shall have one (1) year, beginning the effective date of these Regulations to complete the establishment of their Cybersecurity Units.

C. The Cybersecurity Unit shall be managed by a senior staff who shall have overall supervision and accountability for Cybersecurity. He or she shall assign clear roles and responsibilities for Cybersecurity within the entity.

D. The staff managing the Cybersecurity Unit shall have advanced certification and experience in cybersecurity principles and practices.

E. In line with international best practice, Telecommunications Service Providers shall ensure the identification of individuals having access to their premises/facilities by introducing mandatory identifiers (badges).

7.2 Risk Identification

A. All Telecommunications Service Providers shall:

i. Establish and maintain an updated Baseline Configurations and inventory of all Digital Assets, including hardware, software, firmware, and documentations. The inventory shall contain information about all users and accounts in systems and applications;

ii. Conduct comprehensive risk assessments annually and after significant ICT changes;

iii. Identify and document vulnerabilities, threats, and current controls or safeguards in place to mitigate inherent risks; and

iv. Evaluate the risks of third-parties connecting to their networks, and ensure the third-parties meet the purpose and intent of these regulations.

7.3 Protection of Critical Digital Assets and Infrastructure

A. All Telecommunications Service Providers shall:

i. Implement robust Identity and Access Management (IAM) policies and controls, including Multi-Factor Authentication (MFA);
ii. Deploy measures to safeguard Telecommunications Service Providers' premises from unauthorized access, intrusions, disruptions, damages, and other threats;
iii. Ensure ICT Systems and data are logically organized and segmented according to business criticality and importance;
iv. Encrypt sensitive data both in transit and at rest using industry standards and technologies;
v. Secure Personal Data or Personal Identifiable Information (PII) when collected, processed, transmitted and stored, with industry standards and technologies. Personal data or PII shall not be shared without expressed permission of the owners, and shall be stored primarily inside Liberia's natural boundary;
vi. Provide regular Cybersecurity awareness for all employees; and
vii. Deploy network and web application firewalls, intrusion detection/prevention systems (ID/PS), antivirus software and other protective tools.

7.4 Data Protection and Privacy

A. All Telecommunications Service Providers shall adopt technical and organizational measures to protect consumer data pursuant to Part II, Section 13 of the Telecommunications Consumer Protection Regulations.

7.5 Detection of Cybersecurity Incidents

A. All Telecommunications Service Providers Shall:

i. Establish continuous monitoring systems to detect anomalies;

ii. Conduct Penetration Testing to identify security threats and vulnerabilities at least once a year;

iii. Maintain logs of security events for at least 12 months; and

iv. Regularly assess and mitigate vulnerabilities in accordance with their Service Level Agreement (SLA).

7.6 Incident Response

A. All Telecommunications Service Providers shall:

i. Develop, and annually test, maintain, and update Incident Response Plans (IRPs). The IRP shall be filed with the LTA;

ii. Notify the LTA within 24 hours and customers/subscribers within 72 hours of security breaches and major Cybersecurity Incidents involving Critical Information Infrastructure (CII); and

iii. Contain Cybersecurity Incidents promptly and document response efforts according to the IRP.

7.7 System Recovery

A. All Telecommunications Service Providers shall develop, and annually test, maintain, and update Disaster Recovery and business continuity plans. The Disaster Recovery and Business Continuity Plans shall be filed with the LTA;

7.8 System Monitoring

A. Telecommunications Service Providers are required to implement automated tools for continuous monitoring of their networks, with real-time threat detection.

B. The LTA shall have access to anonymized monitoring data for systemic risk analysis when required.

C. Regular Audits by Telecommunications Service Providers shall be done to assess compliance with Baseline Framework objectives including risk management practices, data protection and incident response capabilities.

7.9 Reporting

A. Telecommunications Service Providers shall submit semiannual reports detailing:

i. Security updates and patches applied;

ii. Detected vulnerabilities and corrective actions taken; and

iii. Incident logs, including near misses, with anonymized data for analysis.

8.0 The Role of the LTA

8.1 Assessing the Effectiveness of Cybersecurity Programs

A. The LTA shall:

i. Regularly evaluate the effectiveness of Telecommunications Service Providers' cybersecurity programs as stipulated in Section 7.0 of these regulations;

ii. Perform periodic random spot checks of Telecommunications Service Providers' compliance as stipulated in Section 7.0 of these regulations;

iii. Evaluate the effectiveness of Telecommunications Service Providers' Disaster Recovery programs; and

iv. Conduct unannounced random examinations to ensure compliance with these Regulations and applicable guidelines. Examinations may focus on one or more provisions of these Regulations, and may include vulnerability assessments, Penetration Testing, process audit, and reviews of Telecommunications Service Providers' Incident Response and Disaster Recovery Plans.

8.2 Establishment of LTA Computer Emergency Response Team (CERT)

A. The LTA shall establish a CERT to respond to Cybersecurity Incidents within the Telecommunications Sector.

B. The CERT shall:

i. Be staffed with personnel with certification and experience in Cybersecurity principles and practices;

ii. Provide a platform for information sharing to enhance safety of the Telecommunications Sector in line with international best practice; and

iii. Ensure the protection and privacy of Personal Data.

C. The responsibilities of the CERT shall include to:

i. Act as the central coordinating body for handling major Cybersecurity Incidents.

ii. Maintain a 24/7 cyber incident hotline for reporting and escalation.

iii. Triage and investigate cybersecurity data breaches and coordinate with relevant national Cybersecurity bodies to drive national response efforts.

8.3 Dispute Resolution

A. Any dispute arising as the result of the enforcement of these Regulations shall be settled in accordance with the LTA's Regulations for the Treatment of Confidentiality, Dispute Resolution, Compliance and Enforcement 2009 (LTA-REG-0002).

8.4 Stakeholders Collaboration

A. Recognizing the global nature of cyber threats, the LTA shall facilitate information sharing and collaboration between Telecommunications Service Providers, governmental agencies, other national stakeholders, and international cybersecurity organizations.

B. Pursuant to Section 8.4 (A) of these regulations, the collaboration shall include participation in regional and international cybersecurity activities, intelligence-sharing initiatives, vulnerability testing, and joint Cybersecurity Simulations and Drills to improve threat detection and mitigation capabilities.

9.0 **Awareness and Capacity Building**

9.1 Awareness

A. The LTA and Telecommunications Service Providers shall regularly conduct nationwide cybersecurity awareness activities to educate the general public of cyber threats and safety measures.

9. 2 Capacity Building

A. The LTA and Telecommunications Service Providers shall ensure continuous training and capacity building of staff working in their respective Cybersecurity Units.

Part III: Violations, Offences and Penalties

10.0 Violations and Penalties

10.1 Establishment of a Cybersecurity Unit

A. Any Telecommunications Service Provider failing to establish a Cybersecurity Unit pursuant to Section 7.1 of these Regulations shall be subject to a fine of not more than three thousand (**USD $3,000**) United States Dollars plus 0.15% of its Annual Gross Revenue of the preceding year.

10.2 Risk Identification Mechanism

A. Any Telecommunications Service Provider failing to put in place a risk identification mechanism as per Section 7.2 of these Regulations shall be subject to a fine of not more than one thousand five hundred ($1,500.00) United States Dollars plus 0.075% of its Annual Gross Revenue of the preceding year.

10.3 Protection of Critical Digital Assets and Infrastructures

A. Any Telecommunications Service Provider failing to put in place mechanism for the protection of Critical Digital Assets and infrastructures as per Section 7.3 of these Regulations shall be subject to a fine of not more than three thousand (**USD $3,000**) United States Dollars plus 0.15% of its Annual Gross Revenue of the preceding year.

10.4 Detection and Reporting of Cybersecurity Incidents

A. Any Telecommunications Service Provider failing to put in place mechanism for the detection and reporting of Cybersecurity Incidents as per Sections 7.4 and 7.5 of these Regulations shall be subject to a fine of not more than one thousand five hundred ($1,500.00) United States Dollars plus 0.075% of its Annual Gross Revenue of the preceding year.

10.5 Incident Response and System Recovery Mechanism

A. Any Telecommunications Service Provider failing to put in place mechanism for incident response and system recovery as per Sections 7.6 and 7.7 of these Regulations shall be subject to a fine of not more than two thousand (2,000.00) United States Dollars plus 0.10% of its Annual Gross Revenue of the preceding year.

10.6 Reporting to the LTA

A. Any Telecommunications Service Provider failing to report to the LTA as per Section 7.8 of these Regulations shall be subject to the below penalties:

i. First offence: Warning notice with a Compliance Order.

ii. Second offense: Fine of up to USD $ 3,000;
iii. Third offense: Fine of up to USD $ 10,000;

iv. Continued non-compliance: Fine up to USD $ 25,000 and possible license suspension or revocation.

10.7 All penalties for violation shall become applicable one year after the effective date of these Regulations.

10.8 Penalties for Telecommunications and Computer Offences

A. Some Telecommunications and Computer related offences have been established in PART XV Section 76 of the Act with corresponding penalties in Section 77 of the Act; hence, they shall apply accordingly.

10.9 Remedial Actions

A. Non-compliant Telecommunications Service Providers shall state the reason(s) for non-compliance and provide detailed mitigation action plans for remediation. On a case-by-case basis, the LTA may provide non-compliant Telecommunications Service Providers a time-frame within which to remedy default. Such time-frame shall take into consideration the size, scope and nature of the default, and the time-frame required for remedy.

B. Irrespective of the remedial action taken pursuant to Section 10.9 (A) above, the appropriate penalties for non-compliance shall still apply. However, non-

compliant Telecommunications Service Providers demonstrating significant improvement within the stipulated time-frame may qualify for reduced penalties.

Part VI: Amendment and Entry into Force

11.0 Amendment

11.1 The LTA may review or amend these Regulations at any time it deems necessary.

11.2 In conducting a review or amendment of these Regulations, the LTA shall consult with stakeholders, external advisory groups or other subject matters experts.

11.3 The LTA may issue additional Rules, Orders, or Notices on any aspect of these Regulations. Such rules, Orders or Notices shall be of general application or specific to a Telecommunications Service Provider from time to time.

12.0 Entry into Force

12.1 These Regulations shall come into effect on the day published.

DONE BY THE LIBERIA TELECOMMUNICATIONS AUTHORITY IN MONROVIA, LIBERIA ON THIS 13th DAY OF JANUARY 2026

Emmanuel J. Payegar
Commissioner

Patrick R. Honnah
Commissioner

Angela Cassell Bush
Commissioner

Ben A. Fofana
Commissioner

Clarence Kortu Massaquoi
CHAIRMAN