

The intro of the Nat Cybersecurity System: a significant step strengthening Mozambique's digital resilience via the approval of Law No. 13/2026, 1Jul, 2026

Law No. 13/2026, of July 1, enacting the Cybersecurity Act, was passed by the Assembly of the Republic on April 29, 2026, promulgated by the President of the Republic, Daniel Francisco Chapo, on June 10, 2026, and published in the Official Gazette, Series I, No. 123, dated July 1, 2026. This law responds to the growing digitization of society and the increase in threats to national cyberspace, aiming to establish a legal framework for the protection of data communication networks, information systems, and critical infrastructure, with the goal of strengthening the digital security of citizens, institutions, and the State.

In this context, there is a need to strengthen the country's digital resilience and to establish effective mechanisms for prevention, detection, response, and recovery in the event of cybersecurity incidents. Pursuant to Article 2, the scope of application of the law covers the Public Administration and the Private Sector, Critical Infrastructure Network Operators, Intermediary Service Providers, Digital Service Providers, Essential Services Network Operators, Cybersecurity Service Providers, Digital Platform Operators, Electronic Communications Operators, as well as individuals and other entities that use data communication networks and information systems.

1. Objectives of the Law

The purpose of this Law is to establish the legal framework applicable to cybersecurity, with a view to guaranteeing the security of the State, its institutions, and its citizens, as well as ensuring the protection of data communication networks, information systems, and critical infrastructure in cyberspace. Pursuant to Article 4, the law is governed by the following principles: (i) collaboration and cooperation; (ii) protection of human rights; (iii) value chain; (iv) transparency; (v) disclosure of vulnerabilities; (vi) accountability; (vii) integrity; (viii) legality; (ix) proportionality; (x) necessity; and (xi) privacy.

2. Establishment of the National Cybersecurity System and Obligations

One of the main innovations of the law is the creation of the National Cybersecurity System, composed of the following bodies, pursuant to Article 6: (i) the National Cybersecurity Council (CNSC), a multisectoral body chaired by the Prime Minister, responsible for political and strategic coordination in the area of cybersecurity (Article 7); (ii) the National Cybersecurity Authority, whose functions are carried out by the National Regulatory Authority for Information and Communication Technologies (), which is responsible for regulating, supervising, monitoring, and imposing sanctions in the field of cybersecurity (Articles 10 and 11); and (iii) the National Cybersecurity Incident Response Team (nCSIRT.MZ), responsible for operational and strategic coordination in the prevention of and response to cyber incidents, operating within the Information and Communication Technologies Regulatory Authority (Article 13). In the event of a state of siege or a state of emergency, the functions of the National Cybersecurity Authority are assumed by the Cybersecurity Coordination Center of the Defense and Security Forces (Article 12).

In turn, the law establishes a set of obligations for the operators and service providers covered by it, including the adoption of cybersecurity risk management measures, incident prevention and response mechanisms, system recovery procedures, and data and communications protection, pursuant to Articles 17, 19, 21, 23, 25, 27, 29, 31, and 33. These entities are also required to maintain confidentiality regarding all communications transmitted by their users; however, they may provide communications containing criminal content or that threaten national security to the competent authorities, subject to a duly substantiated judicial or administrative decision.

In various sectors considered critical or essential, the creation of institutional Cybersecurity Incident Response Teams (CSIRTs) is also required, as well as registration with the National Cybersecurity Authority, pursuant to Articles 17, 19, 21, 23, 25, 27, 29, 31, and 33. The National CSIRT Network, provided for in Article 15, serves as the forum for exchanging information on cyber incidents among the National CSIRT, sectoral CSIRTs, and institutional CSIRTs, operating under the coordination of the Information and Communication Technologies Regulatory Authority through the National CSIRT.

3. Security of Networks and Information Systems and Minimum Security Requirements

Chapter III of the Law establishes the security regime for networks and information systems, requiring the entities covered to ensure the integrity, confidentiality, and privacy of communications

through the implementation of logical and physical security measures (Article 34). The security of traffic and location data, the preservation of evidence, and the retention of data for a minimum period of 1 year are also regulated (Articles 37 through 40).

Chapter IV establishes mandatory minimum security requirements for all entities covered by the law, pursuant to Article 48, which include, in particular: the existence of an information security policy, a cyber risk management methodology, incident reporting procedures, mechanisms for preventing, correcting, or mitigating risk, backup and recovery infrastructure, internal audit mechanisms, as well as the appointment of an information security officer and the creation of an incident detection and response team. The specific security requirements applicable to each category of operator and service provider are detailed in Articles 50 through 56.

4. Cybersecurity Incident Notification and Vulnerability Disclosure

Chapter IV, Section II, establishes the mandatory reporting regime for cybersecurity incidents with a significant impact. Covered entities are required to report incidents to their respective sectoral CSIRT and the National CSIRT within the timeframes set by the National Cybersecurity Authority; incident response and resolution reports must include information on the causes of the incident, the time taken to resolve it, the measures implemented, and the resulting impact, in accordance with Articles 57 through 65.

Article 66 enshrines the principle of responsible vulnerability disclosure, allowing any natural or legal person to report, publish, or disclose vulnerabilities, provided that such disclosure is made in good faith, without incurring liability, and provided that the conditions set forth in the law are met, namely the granting of a minimum period of 90 days for the vulnerability to be corrected prior to its publication or disclosure.

5. Cybersecurity Fund and Penalty System

Chapter V establishes the Cybersecurity Fund (FSC), managed by the National Cybersecurity Authority, with the aim of strengthening national cybersecurity. Pursuant to Article 67(3), entities registered and licensed to provide ICT services contribute to the FSC, and Article 70(c) sets a

contribution of 1% of the previous year's gross revenue for entities within the National Cybersecurity System that are licensed to provide cybersecurity services (Articles 67–71). Chapter VI establishes the framework for supervision, inspection, administrative offenses, and sanctions, providing, in particular, for the imposition of fines that, in cases of noncompliance with security requirements, may range from 90 to 160 times the minimum civil service salary, and between 80 and 100 minimum wages in cases of failure to comply with incident reporting obligations (Article 76). The law takes effect 90 days after its publication, and the Government must issue implementing regulations within 180 days (Articles 79 and 80).

6. **Considerations**

The Cybersecurity Law represents a fundamental step in consolidating Mozambique's legal framework regarding digital governance and the protection of cyberspace. The law introduces comprehensive mechanisms for prevention, detection, response, and recovery in the face of cyber threats, supported by a dedicated institutional architecture and an effective sanctions regime.

The law thus seeks to promote a culture of cybersecurity, ensure the resilience of the country's critical infrastructure and services, and align Mozambique's legal framework with international best practices in the field of digital security, thereby helping to strengthen the confidence of citizens, businesses, and the State in the national digital ecosystem.

For further information and updates please contact JLA Advogados, the LEX Africa member in Mozambique, on maputo@jlaadvogados.com or visit <https://www.jlaadvogados.com>.