

Ethiopia Enacts the Critical Infrastructure Cybersecurity Proclamation No. 1426/2026

👤 Kiya Tsegaye 📅 September 29, 2026 ⌚ 7 min read

For the first time, Ethiopia has a dedicated law protecting critical infrastructure against cyberattacks: designation of infrastructure across twelve sectors, mandatory owner security programs, 48-hour incident reporting, licensing of cybersecurity providers, and fines of up to Birr 2,000,000 with imprisonment for serious breaches.

Ethiopia has adopted Proclamation No. 1426/2026, published in the Federal Negarit Gazette (32nd Year, No. 41) on 21 July 2026. It creates, for the first time, a dedicated legal regime for protecting the country's most sensitive public and private infrastructure against cyberattacks, and places the Information Network Security Administration (the "Administration") at the centre of oversight. The Proclamation enters into force one year after publication, meaning on or about July 2027. As Kiya & Associates Law Office, we have prepared this note to explain what changes and what businesses should be doing now.

Who Is Covered?

"Critical infrastructure" means any public or private infrastructure or institution whose disruption through a cyberattack would significantly harm national security or national interests. The Proclamation identifies twelve sectors, including ICT, finance, security, transport, education, health, water and energy, government services, disaster management, agriculture, trade and industry, and allows the Administration to add more. Coverage is not automatic: the Administration designates specific infrastructure by directive, applying criteria such as economic and social impact, effect on national security and sovereignty, and the degree of interconnection with other sectors, and notifies the owner. Designation can later be withdrawn if the criteria cease to be met. The law also applies to designated infrastructure located outside Ethiopia and to anyone supplying cybersecurity products or services.

New Duties for Owners of Designated Infrastructure

Owners must adopt their own cybersecurity programs aligned with national frameworks, implement mandatory frameworks issued or recognized by the Administration, classify and protect critical assets, and carry out regular risk and impact assessments. They must take part in an annual national cybersecurity risk survey, hold current cyber audit and inspection certificates, and correct any weaknesses within the time set by the Administration. Any new or upgraded ICT system, whether bought, donated or developed, needs security clearance before it is put into use.

Owners must also secure their technology supply chain, hire certified cybersecurity professionals, run drills and training, and ensure that staff with access to critical resources obtain government security clearance. Most notably, a cyber incident must be reported to the National Computer Emergency Response Centre within 48 hours, and its directions followed. Owners may delegate these duties to a licensed provider, except for infrastructure the Administration excludes from delegation on national security grounds.

Licensing of Providers and Accreditation of Professionals

Supplying cybersecurity products or services now requires a licence from the Administration. Applicants must be legally established, hold security clearance, have a permanent address in Ethiopia, meet capital, guarantee, personnel and technology requirements set by directive, and have no conviction for fraud, corruption or breach of trust. Licences may not be transferred, lent or shared, may be suspended for up to sixty days pending investigation, and are revoked for fraud, misuse, or breach of the law. Professionals working in critical infrastructure will also need certification or accreditation under a forthcoming directive.

Cybersecurity Fund

A permanent Critical Infrastructure Cyber Security Fund is established to finance programs, research, training and enabling systems. It will be fed by contributions from critical infrastructure owners, to be fixed by a Council of Ministers regulation, together with voluntary donations, service fees and administrative fines. Owners should therefore anticipate a recurring financial contribution.

Penalties and Criminal Liability

Intentional breaches by an owner attract administrative fines:

- Birr 500,000 to 1,000,000 for failing to implement mandatory frameworks on time;
- Birr 1,500,000 to 2,000,000 for failing to report an incident within 48 hours or to take corrective action, or for failing to cooperate with audits;
- Birr 800,000 to 1,000,000 for not remedying audit findings or for using ICT systems that were not inspected; and

Unlicensed service provision, or breach of a licensee's duties, carries a fine of Birr 1,200,000 to 2,000,000. A repeat offence attracts triple the maximum fine, while a first offence causing no damage may be met with a written warning only. Negligent breaches attract reduced fines, although the Amharic and English texts describe the extent of the reduction slightly differently.

Individually, officers, employees, managers and owners who intentionally commit the core breaches face simple imprisonment of up to one year. Where the breach interrupts or damages critical services, compromises integrity or confidentiality, or harms national security, public health, life or the environment, the sentence rises to rigorous imprisonment of seven to ten years. Negligent commission carries up to six months' simple imprisonment, or three to five years' rigorous imprisonment where serious harm results.

Complaints and Appeals

A written complaint against the Administration's implementation of the law must be filed within thirty days of the cause arising, and a decision is due within fifteen working days. Further grievances go to a board of government and private sector representatives to be established by regulation, and its decisions may be appealed to the competent court within sixty days.

What This Means Going Forward

The Proclamation relies heavily on directives and regulations still to come, including designation of critical infrastructure, frameworks, licensing rules, fund contributions and complaint procedures. Businesses in the listed sectors should use the one-year transition to assess whether they are likely to be designated, map their assets and vendors, establish an incident reporting process capable of meeting the 48-hour deadline, and review procurement and staffing practices. Cybersecurity providers should prepare for licensing.

Kiya & Associates Law Office will monitor the implementing instruments and is glad to assist clients with readiness, compliance and licensing.

This article is provided for general informational purposes only and does not constitute legal advice. For guidance specific to your circumstances, please contact Kiya & Associates Law Office.