የኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ

ፌደራል ነጋሪት ጋዜጣ

FEDERAL NEGARIT GAZETTE

OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

፴፪ኛ ዓመት ቁጥር ፵፩
አዲስ አበባ ሐምሌ ፲፬ ቀን ፪ሺ፲፰

በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ የሕዝብ ተወካዮች ምክር ቤት ጠባቂነት የወጣ

32th Year No. 41
ADDIS ABABA, 21th July, 2026

ማውጫ

አዋጅ ቁጥር ፩ሺ፬፻፳፮/፪ሺ፲፰

የቁልፍ መሰረተ ልማቶች የሳይበር ደህንነት አዋጅ……...............................ገጽ ፲፱ሺ፰፻፳፰

Content

Proclamation No. 1426/2026

Critical Infrastructure Cybersecurity Proclamation ……………….Page 19828

አዋጅ ቁጥር ፩ሺ፬፻፳፮/፪ሺ፲፰

የቁልፍ መሠረተ ልማቶች የሳይበር ደህንነት ለመጠበቅ የወጣ አዋጅ

በቁልፍ መሠረተ ልማቶች ላይ የሚነጣጠሩ የሳይበር ጥቃቶች በሀገሪቱ ምጣኔ ሃብት፣ ማህበራዊ መስተጋብር፣ ብሔራዊ ደህንነት፣ ሰላምና መረጋጋት እንዲሁም ሉዓላዊነት ላይ አሉታዊ ተፅዕኖ የሚፈጥሩ በመሆናቸው፤

በቁልፍ መሰረተ ልማቶች እና መሰረተ ልማቶቹ በሚይዟቸው ኢንፎርሜሽኖች እና ዳታዎች ላይ እየጨመሩ የመጡ የሳይበር ደህንነት ተጋላጭነቶችና ስጋቶችን መቀነስና መከላከል አስፈላጊ ሆኖ በመገኘቱ፤

የሳይበር ጥቃት ስጋትን መሠረት ያደረገ የቁልፍ መሠረተ ልማቶች ልየታ በማድረግ የሀገሪቱን ሀብት አቀናጅቶ ለመምራት የሚያስችል የሳይበር ደህንነት ጥበቃና ቁጥጥር ማድረግ አስፈላጊ ሆኖ በመገኘቱ፤

PROCLAMATION NO. 1426/2026

CRITICAL INFRASTRUCTURE CYBER SECURITY PROTECTION PROCLAMATION

WHEREAS, it has become evident that cyberattacks targeting critical infrastructure harm the country's economy, social interaction, national security, peace and stability, and sovereignty;

WHEREAS, it is imperative to mitigate and prevent the growing cybersecurity vulnerabilities and threats that jeopardize critical infrastructure and the information and data they possess;

WHEREAS, it has become necessary to establish a cybersecurity assurance and control, based on cybersecurity risk based identification of critical infrastructure, to manage national resources and ensure their resilience;

ለቁልፍ መሰረተ ልማቶች የሳይበር ደህንነት ጥበቃ በባለድርሻ አካላት መካከል የተቀናጀ፣ ውጤታማና ፈጣን የመረጃ ልውውጥ እና የሳይበር ክስተቶችን ለማጋራትና ለመግታት የሚያስችል ስርዓት መፍጠር አስፈላጊ ሆኖ በመገኘቱ፤

ውስብስብ፣ ተለዋዋጭ እና ከፍተኛ የሆነ ወድድር ባለበት የሳይበር ምህዳር ውስጥ የሚደረግ የሳይበር ደህንነትን የማረጋገጥ ተግባር ከፍተኛ የሆነ የካፒታል አቅምን የሚጠይቅ በመሆኑ፤ ለቁልፍ መሠረተ ልማቶች ጥበቃ የሚውል አስተማማኝ ሀገራዊ የፋይናንስ አቅም መፈጠር አስፈላጊ ሆኖ በመገኘቱ፤

ቁልፍ መሠረተ ልማቶችን በሚያስተዳድሩና የሳይበር ደህንነት ጥበቃን በሚያደርጉ አካላት ላይ ግልፅ ኃላፊነትና ተጠያቂነት መፍጠር አስፈላጊ ሆኖ በመገኘቱ፤

በመሆኑም በኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ ህገ መንግሥት አንቀጽ ፶፭ ንዑስ አንቀፅ (፩) መሠረት የሚከተለው ታውጇል።

ክፍል አንድ
ጠቅላላ ድንጋጌዎች

፩. አጭር ርዕስ

ይህ አዋጅ “የቁልፍ መሰረተ ልማቶች የሳይበር ደህንነት አዋጅ ቁጥር ፩ሺ፬፻፳፮/፪ሺ፲፰” ተብሎ ሊጠቀስ ይችላል፡፡

WHEREAS, it is necessary to establish a system for integrated, effective, and rapid information exchange among stakeholders to ensure critical infrastructure cybersecurity, enabling the sharing and mitigation of cyber incidents;

WHEREAS, ensuring cybersecurity in a complex, dynamic, and highly competitive cyber environment requires significant capital investment; and whereas, it is essential to create a reliable national financial capacity for the protection of critical infrastructure;

WHEREAS, it is necessary to impose clear responsibilities and obligations on the entities that manage critical infrastructure and provide cybersecurity protection;

NOW, THEREFORE, this Proclamation has been proclaimed in Pursuant to Article 55, Sub-Article (1) of the Constitution of the Federal Democratic Republic of Ethiopia.

PART ONE
GENERAL PROVISIONS

1. Short title

This Proclamation may be cited as the "Critical Infrastructure Cybersecurity Proclamation No. 1426/2026."

፪. ትርጓሜ

የቃሉ አገባብ ሌላ ትርጉም የሚያሰጠው ካልሆነ በስተቀር በዚህ አዋጅ ውስጥ፡-

፩/ **"ቁልፍ መሰረተ ልማት"** ማለት ለሳይበር ጥቃት ከተጋለጠ በብሔራዊ ደህንነትና ብሔራዊ ጥቅሞች ላይ ጉዳት የሚያስከትል የመንግስት ወይም የግል መሰረተ ልማቶች እና ተቋማትን ያካትታል፤

፪/ **"የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ስርዓት"** ማለት የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ምርቶች፣ አገልግሎቶች፣ ኔትወርኮች፣ የአሰራር ስርዓቶች፤ ሃርድዌሮችን፣ ሶፍትዌር መተግበሪያዎች ወይም ስልተ ቀመሮች ያካትታል፤

፫/ **"የሳይበር ምህዳር"** ማለት እርስ በርሳቸው የተሳሰሩ የኢንፎርሜሽን መሰረተ ልማቶች፣ ኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ስርዓቶች፣ ኢንፎርሜሽንን ወደ እውቀት የሚቀይርና የሚጠቀም የሰው ሃይል እንዲሁም ተቋማዊና ማህበረሰባዊ ባህልን ያካተተ ምናባዊ ባህሪ ያለው ምህዳር ነው፤

፬/ **"የሳይበር ክስተት"** ማለት የሳይበር ደህንነት እና ተቀባይነት ካላቸው የአጠቃቀም ፖሊሲዎች ወይም ከተለመዱ የደህንነት አሰራሮች ያፈነገጠ ጥሰት ወይም ሊከሰት የሚችል የጥሰት ስጋትን ሲሆን፤ ማንኛውም የኔትወርክ፣ የመረጃ ሥርዓቶች ወይም ጥበቃ የሚያስፈልጋቸው ዳታዎችን ምስጢራዊነት፣ ትክክለኛነት፣ ተደራሽነት፣ እውነተኛነት ወይም የማይካድነት ላይ ጉዳት የሚያደርስ አፍራሽ የሳይበር ደህንነት ክስተት ነው፤

2. Definitions

In this Proclamation, unless the context otherwise requires:

1/ **"Critical Infrastructure"** any public or private infrastructure or institution the disruption or compromise of which due to a cyberattack would have a significant negative impact on national security or national interests.

2/ **"Information Communication Technology System"** means information communication technology products, services, networks, operating systems, hardwares, software applications, and algorithms;

3/ **"Cyberspace"** means the interconnected environment comprising information infrastructure, information and communication technology systems, the human element that generates and uses information, and the institutional and societal culture that shapes it;

4/ **"Cyber incident"** means a violation or imminent threat of violation of security and acceptable use policies, or standard security practices; or any adverse cyber security event that compromises the confidentiality, integrity, availability, authenticity, or non-repudiation of a network, information systems, or sensitive data;

፭/ **“የሳይበር ጥቃት”** ማለት በሳይበር ምህዳር የሚፈጸም ቁልፍ መሰረተ ልማት የማስተጓጎልን፣ ማቋረጥን፣ የማጥፋትን፣ ማፈንን፣ ያለፈቃድ ብርበራን፣ የመረጃ ስርቆትን፣ እንዲሁም የኢንፎርሜሽን ምስጢራዊነት፣ ተደራሽነት ወይም ምልዑነትን የሚያሳጡ ጥቃቶችን ያካትታል፤

5/ **"Cyberattack"** means any attack conducted in cyberspace that disrupts, interrupts, suppresses, infiltrates, steals data, and otherwise compromises critical infrastructure;

፮/ **“የቁልፍ መሰረተ ልማት ባለቤት”** ማለት የቁልፍ መሰረተ ልማት ባለቤት ወይም በቁልፍ መሰረተ ልማት ባለቤት መሰረተ ልማቱን እንዲያስተዳደሩ የተወከሉ ሰዎችን ይጨምራል፤

6/ **"Critical Infrastructure Owner"** means the legitimate owner of critical infrastructure or persons delegated by the critical infrastructure owner to manage the infrastructure;

፯/ **“ሀብት”** ማለት ካልተገባ ወይም ህገወጥ ተደራሽነት፣ ጥቅም፣ ይፋ መሆን፣ ለውጥ፣ ውድመት እና ተጋላጭነት ሊጠበቅ የሚገባው ማንኛውም የኢንፎርሜሽን ኮምኒኬሽን ቴክኖሎጂ ስርዓት ወይም ቁስ ነው፤

7/ **"Asset"** means any information and communication technology system or material that must be protected from unauthorized access, use, disclosure, alteration, destruction, and vulnerability in critical infrastructures;

፰/ **“የሳይበር ደህንነት ፕሮግራም”** ማለት በአደጋ ትንተና ላይ የተመሰረተ የሳይበር ደህንነትን ለማረጋገጥ እንዲተገበሩ የሚወጡ የስትራቴጂ፣ የታክቲክ፣ የኦፕሬሽን እና የአሠራር እርምጃዎች እንዲሁም የአስተዳደር መዋቅሮችን ያጠቃልላል፤

8/ **"Cybersecurity Program"** means strategic, tactical, and operational measures to be implemented to ensure cybersecurity based on risk analysis, as well as governance structures;

፱/ **“የሳይበር ደህንነት ማዕቀፍ”** ማለት አስተዳደሩ ወይም ቁልፍ መሰረተ ልማቶች እንዲያወጧቸው የሚጠበቁ የሳይበር ደህንነትን ለመምራት እና ለማስተዳደር የሚያስችሉ ስትራቴጂያዊ፣ የአተገባበር፣ የሂደት፣ የአሰራር ስርዓት፣ የስልት እና ሌሎች መሰል ሀገራዊ ወይም ዘርፍ ተኮር አስገዳጅ ወይም አስገዳጅ ያልሆኑ ማዕቀፎች ናቸው፤

፲/ **“የሳይበር ደህንነት ፍተሻና ግምገማ”** ማለት የሳይበር ደህንነት ማዕቀፎች መሠረት ኢንፎርሜሽን ኮምኒኬሽን ቴክኖሎጂ ስርዓቶችን የቅድመ ልማት፣ ቅድመ ግዥ እና ቅድመ ትግበራ ላይ የሚደረግ ፍተሻ እና ግምገማ የማድረግ ተግባር ነው፤

፲፩/ **“የደህንነት ማረጋገጫ”** ማለት በቁልፍ መሰረተ ልማት ውስጥ የሚሰራ ሰራተኛ ወይም ኃላፊ ለታጨበት ወይም ለተመደበበት የስራ ሃላፊነት አስፈላጊ ሙያዊ ስብዕና እና ስነ ምግባር ያለው መሆኑን የማጥናትና የማጣራት ሂደት ነው፤

፲፪/ **“የሳይበር ደህንነት ኦዲት”** ማለት በቁልፍ መሰረተ ልማቶች ላይ ተጋላጭነትን ለማወቅ የዘልቆ ገብ ፍተሻ ተግባራትን ማከናወን እና ሀገራዊ የሳይበር ደህንነት ማዕቀፎችን መሠረት በማድረግ የቁልፍ መሰረተ ልማቶችን የሳይበር ደህንነት ስርዓት በመገምገም እንደአስፈላጊነቱ የእርምት እርምጃዎች እንዲወሰዱ ማድረግን ይጨምራል፤

9/ **"Cybersecurity Framework"** means strategic, implementation, process, procedure, methodology, and other similar frameworks for leading and managing national or sector-specific cybersecurity issued by the Administration and binding and/or non-binding documents issued by the Administration or required by institutions to issue them;

10/ **"Cybersecurity Inspection and Evaluation"** means the conduct of inspections and evaluations of pre-development, pre-purchase, and pre-implementation information communication technology systems under national cybersecurity frameworks;

11/ **"Security Clearance"** means the process of studying and checking whether a person has the responsibilities, integrity, and essential personality of the job to which he is nominated or assigned;

12/ **"Cybersecurity Audit"** means performing penetration inspection activities to detect vulnerabilities in critical infrastructure and evaluating the cybersecurity systems of critical infrastructure in accordance with national cybersecurity frameworks to take corrective actions as appropriate;

፲፫/ **"ብሔራዊ ደንገተኛ የኮምፒውተር አደጋ ምላሽ መስጫ ማዕከል"** ማለት በቁልፍ መሰረተ ልማቶች ላይ የሚሰነዘር ጥቃትን ለመከላከል እንዲቻል የጥቃት አደጋዎችን አስቀድሞ የመለየት፣ የመተንተን፣ ዜጎችንና ተቋማትን የማስጠንቀቅ፣ መወሰድ ስለሚገባቸው እርምጃዎች ምክርን የማቅረብ፣ የማገገሚያ መንገዶችን የመዘየድ እና በዚህ ዘርፍ ሀገራዊ እና ዓለም አቀፋዊ ቅንጅትን እንዲፈጠር የማስቻል ተግባራትን የሚያከናውን ማዕከል ነው፤

፲፬/ **"የሳይበር ደህንነት አገልግሎት ሰጪ"** ማለት በዚህ አዋጅ መሠረት የሳይበር ደህንነት ምርት ወይም አገልግሎት ለመስጠት ፈቃድ የተሰጠው ሰው ነው፤

፲፭/ **"የሳይበር ደህንነት ባለሙያ"** ማለት በዚህ አዋጅ መሠረት የሳይበር ደህንነት ተግባራትን እንዲያከናውን እውቅና የተሰጠው ሰው ነው፤

፲፮/ **"የሳይበር ደህንነት ምርትና አገልግሎት"** ማለት የሳይበር ጥቃትን ወይም የኢንፎርሜሽንን ምስጢራዊነት፣ ምልዑነት እና ተደራሽነት ስጋቶችን ለመቀነስ እና ለማስተዳደር የሚሰጡ ምርቶች ወይም አገልግሎት ነው።

፲፯/ **"አስተዳደር"** ማለት የኢንፎርሜሽን መረብ ደህንነት አስተዳደር ነው፤

13/ "**National Computer Emergency Response Center**" means a center that performs the functions of early detection of threats to critical infrastructure, analysis, warning citizens and institutions, providing advice on actions to be taken, planning recovery measures, and facilitating national and international coordination in this area in order to prevent attacks on critical infrastructure;

14/ "**Cybersecurity Service Provider**" means a person licensed to provide cybersecurity products or services in accordance with this Proclamation;

15/ **"Cybersecurity Professional**" means a person accredited to carry out cybersecurity activities under this Proclamation;

16/ "**Cybersecurity Product and Service"** means any hardware, software, algorithm, or service offered for the purpose of protecting information, equipment, devices, computers, computer resources, communication devices, and data stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction, including offerings for cyber forensics and cyber incident response;

17/ **"Administration"** means the Information Network Security Administration;

፲፰/ **“ሰው”** ማለት የተፈጥሮ ሰው ወይም በሕግ የሰውነት መብት የተሰጠው አካል ነው፤

፲፱/ ማንኛውም በወንድ ፆታ የተገለፀው ሴትንም ይጨምራል፡፡

፫. <u>የተፈፃሚነት ወሰን</u>

ይህ አዋጅ በመላው የኢትዮጵያ ግዛት ውስጥ ሆነ ከሀገር ግዛት ውጭ ልየታ በተደረገላቸው የሀገሪቱ የቁልፍ መሠረተ ልማቶች እንዲሁም የሳይበር ደህንነት ምርት ወይም አገልግሎት በሚያቀርቡ ሰዎች ላይ ተፈፃሚ ይሆናል።

<u>ክፍል ሁለት</u>
<u>ቁልፍ መሰረተ ልማቶችን ስለመለየት እና ስለመጠበቅ</u>

፬. <u>የቁልፍ መሰረተ ልማት ዘርፎች</u>

፩/ የሚከተሉት የቁልፍ መሰረተ ልማት ዘርፎች ተብለው በዚህ አዋጅ ተለይተዋል፡-

ሀ) የኢንፎርሜሽን ቴክኖሎጂ እና ኮሚኒኬሽን፤

ለ) የፋይናንስ፤

ሐ) የፀጥታና ደህንነት፤

መ) የትራንስፖርት፤

ሠ) የትምህርት፤

ረ) የጤና፤

ሰ) የውሃና ኢነርጂ፤

ሸ) የመንግሥት አገልግሎቶች፤

ቀ) የአደጋ መከላከል አገልግሎቶች፤

በ) ግብርና፤

ተ) ንግድ፤

ቸ) ኢንዱስትሪ፤

18/ **"Person"** means a natural person or a person who has been granted the right to a person by law;

19/ Any expression of the male gender also includes a woman.

3. <u>Scope of Application</u>

This Proclamation shall apply to designated critical infrastructures of the country located within or outside the territory of Ethiopia, as well as to persons providing cybersecurity products or services.

<u>PART TWO</u>
<u>IDENTIFYING CRITICAL INFRASTRUCTURE AND PROTECTION</u>

4. <u>Identify Critical Infrastructure</u>

1/ The following critical infrastructure sectors are identified in this Proclamation:

a) Information Technology and Communication;

b) Finance;

c) Security and Safety;

d) Transport;

e) Education;

f) Health;

g) Water and Energy;

h) Government Services;

i) Disaster Management Services;

j) Agriculture;

k) Trade;

l) Industry;

፪/ የዚህ አንቀፅ ንዑስ አንቀፅ (፩) እንደተጠበቀ ሆኖ አስተዳደሩ ተጨማሪ ቁልፍ መሰረተ ልማት ዘርፎችን ሊለይ ይችላል፡፡

፫/ በዚህ አንቀፅ ንዑስ አንቀፅ (፪) መሠረት ቁልፍ መሠረተ ልማትን ለመለየት የሚከተሉት ዝቅተኛ መስፈርቶች መሟላት ይኖርባቸዋል፦

ሀ) የሳይበር ጥቃት ቢደርስበት በምጣኔ ሀብት፣ ማህበራዊ መስተጋብር፣ በማህበረሰቡ የዕለት ተዕለት ኑሮ ላይ አደጋ የሚጥል ሲሆን፤

ለ/ የሳይበር ጥቃት ቢደርስበት በብሔራዊ ደህንነት፣ በሰላምና መረጋጋት፣ በዲፕሎማሲ ወይም በሀገር ደህንነትና ህልውና ላይ አሉታዊ ተፅዕኖ የሚያሳድር ሲሆኑ፤ እና

ሐ) ከፍተኛ ትስስርና መስተጋብር ያላቸውና ጉዳት ቢደርስበት ወደ ሌሎች ቁልፍ መሰረተ ልማት ዘርፎች የሚዛመት ሲሆኑ፤

መ) ሌሎች እንደአስፈላጊነቱ አስተዳደሩ በመመሪያ በሚያወጣቸው አግባብነት ያላቸው መስፈርቶች።

፭. <u>ቁልፍ መሰረተ ልማቶችን ስለመሰየም</u>

፩/ አስተዳደሩ በዚህ አዋጅ አንቀፅ ፬ መሠረት የተለዩ ቁልፍ መሠረተ ልማት ዘርፎች ውስጥ ለሳይበር ጥቃት ተጋላጭ የሆኑ እና በዚህ አዋጅ መሠረት ጥበቃ ሊደረግላቸው የሚገቡ የቁልፍ መሰረተ ልማቶችን በመለየት በመመሪያ ይሰይማል፤ ለመሰረተ ልማቱ ባለቤት ያሳውቃል፡፡

2/ Without prejudice to Sub-Article (1) of this Article, the Administration may identify additional critical infrastructure sectors.

3/ In order to identify critical infrastructure in accordance with Sub-Article (2) of this Article, the following minimum criteria must be met:

a) in the event of a cyberattack, it poses a threat to the economy, social interaction, and daily life of the community;

b) in the event of a cyberattack that adversely affects national security, peace and stability, diplomacy, or national security and sovereignty; and

c) If there is a high level of interconnectedness and interaction, and if the damage occurs, it will spread to other critical infrastructure sectors;

d) Other relevant criteria to be issued by the Administration through Directives, as necessary.

5. <u>Designation of Critical Infrastructure</u>

1/ Drawing from sectors identified in Article 4 of this Proclamaiaton, the Administration shall designate critical infrastructures susceptible to cyber attacks that require protection through a Directive, and notify the critical infrastructure owner.

፪/ አስተዳደሩ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሠረት ቁልፍ መሰረተ ልማት ሲሰይም፤ የሳይበር ደህንነት ማዕቀፎችንና ምርጥ ተሞክሮዎችን መሠረት ያደርጋል፤ የሀገሪቱን የሳይበር ደህንነት ስጋት ተፅዕኖ ይተነትናል፤ ይገመግማል፤ እንዲሁም ወቅታዊ ፍላጎትን መሠረት ያደርጋል፡፡

፫/ በዚህ አንቀፅ መሠረት በቁልፍ መሠረተ ልማትነት የተለየ ተቋም በአዋጁ መሠረት የሚሰጡ የሳይበር ደህንነት ጥበቃ ተግባራት ተጠቃሚ ይሆናል።

፮. <u>ከቁልፍ መሰረተ ልማትነት ስለመሰረዝ</u>

፩/ ቁልፍ መሠረተ ልማት ተብሎ የተሰየመ መሰረተ ልማት በዚህ አዋጅ አንቀጽ ፬ ንዑስ አንቀፅ (፫) ላይ የተዘረዘሩትን መስፈርቶች ማሟላት ሲያቆም አስተዳደሩ ተገቢውን ግምገማ በማድረግ ከቁልፍ መሰረተ ልማትነት ሊሰርዘው ይችላል፤

፪/ ከቁልፍ መሰረተ ልማትነት ለተሰረዘ መሰረተ ልማት በዚህ አዋጅ መሠረት የሚደረገው ጥበቃ ይቋረጣል።

፯. <u>የቁልፍ መሰረተ ልማት ባለቤት ግዴታ</u>

ማንኛውም የቁልፍ መሰረተ ልማት ባለቤት የሚከተሉት ግዴታዎች ይኖሩበታል፡-

፩/ ሀገራዊ የሳይበር ደህንነት ማዕቀፎች መሠረት በማድረግ የራሱን የሳይበር ደህንነት ፕሮግራሞችን የመቅረፅ፤

2/ When designating critical infrastructure under sub article (1) of this Article, the Administration shall analyze and assess the country's cybersecurity risk impact, taking into account cybersecurity frameworks, best practices, and current needs; and shall develop and implement relevant standards.

3/ In accordance with this Article, a specific institution designated as critical infrastructure shall benefit from cybersecurity protection provided in accordance with the Proclamation.

6. <u>Removal of Critical Infrastructure</u>

1/ When an infrastructure designated as critical infrastructure ceases to meet the requirements set out in Sub-Article (3) of Article 4 of this Proclamation, the Administration may remove it after appropriate assessment from critical infrastructure;

2/ For infrastructure that has been removed from critical infrastructure, the protection under this Proclamation shall be terminated.

7. <u>Duty of the Owner of Critical Infrastructure</u>

Any owner of critical infrastructure shall have the following obligations:

1/ To formulate its own cybersecurity programs based on the national cybersecurity frameworks;

፪/ በሀገር አቀፍ ደረጃ የሚወጡ ወይም እንደ ሀገር እውቅና የተሰጣቸውን ዓለም አቀፍ አስገዳጅ የሳይበር ደህንነት ማዕቀፎች ተግባራዊ የማድረግ፤

፫/ በሀገራዊ ህጎችና ፖሊሲዎች እንዲሁም በአስተዳደሩ በሚወጡ ቴክኒካል ፖሊሲ መሠረት ያደረገ የራሱን የሳይበር ደህንነት ማዕቀፍ ማዘጋጀትና ተግባራዊ የማድረግ፤

፬/ አስተዳደሩ በሚያወጣው ስታንዳርድ መሰረት በስሩ የሚያስተዳድራቸውን ሀብቶች የመመደብና የመጠበቅ፤

፭/ አስተዳደሩ በሚዘረጋው ስርዓት መሠረት ወቅታዊ የሳይበር ደህንነት የአደጋ ዳሰሳ እና የተፅዕኖ ትንተና ማድረግ፤

፮/ አስተዳደሩ በየአመቱ በሚያከናውነው ሀገራዊ የሳይበር ደህንነት የአደጋ ዳሰሳ ላይ የመሳተፍና አስፈላጊ መረጃዎችን የማቅረብ፤

፯/ አስተዳደሩ በሚዘረጋው ስርዓት መሠረት የሳይበር ኦዲት እና የሳይበር ፍተሻና ግምገማ ማረጋገጫ ሰርተፍኬት የመያዝና የማሳደስ፤

፰/ በሳይበር ኦዲት ወይም የሳይበር ደህንነት ፍተሻና ግምገማ ግኝት መሠረት በሚሰጠው የጊዜ ገደብ ውስጥ ተገቢውን የእርምት እርምጃ የመውሰድ፤

፱/ በሀገራዊ የሳይበር ደህንነት ማዕቀፍ መሠረት አስፈላጊውን የሳይበር ደህንነት አደረጃጀት የመፍጠር፡፡

2/ Implement mandatory cybersecurity frameworks issued or recognized by the Administration;

3/ Develop and implement its own cybersecurity framework based on policies and laws issued by the Administration;

4/ To classify and protect critical assets in accordance with standard set by the administration;

5/ Conducting regular cybersecurity risk assessments and impact analyses in accordance with system established by the Administration;

6/ To participate in the National Cybersecurity Risk Survey conducted by the Administration annually and to provide relevant information;

7/ Maintain and renew the cyber audit and cyber inspection and evaluation certificate issued by the Administration;

8/ To take appropriate corrective action in accordance with the findings of the Administration's cyber audit or cybersecurity inspection and evaluation;

9/ To create the necessary cybersecurity organizational structure in accordance with the national cybersecurity framework.

፲/ ከአስተዳደሩ የተሰጡ ወይም በአስተዳደሩ እውቅና የተሰጣቸው የሙያ ሰርተፍኬቶችን ያገኙ የሳይበር ደህንነት ባለሙያዎችን የመቅጠር፤ ያሉትን ባለሙያዎች አስተዳደሩ በሚዘረጋው ስርዓት መሠረት የሙያ ብቃት ማረጋገጫ እንዲያገኙ የማድረግ፤

፲፩/ ጥቅም ላይ የሚያውሏቸውን የቴክኖሎጂ ምርቶች አቅርቦት ሰንሰለት ደህንነት ማረጋገጥ፤

፲፪/ አዳዲስ ወይም ተሻሽለው የሚቀርቡ የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ስርዓቶችን በግዥ፣ በስጦታ፣ በማልማት ወይም በማንኛውም መልኩ አግኝተው ከመተግበራቸው በፊት አስተዳደሩ በሚዘረጋው ስርዓት መሠረት ደህንነት ማረጋገጫ የማግኘት፤

፲፫/ አስተዳደሩ በሚዘረጋው ስርዓት መሠረት የሳይበር ጥቃቶችን ክትትል፣ ሪፖርት እና ምላሽ የማድረግ እና ተግባሩን የሚያስተዳድር ማዕከል የማደራጀት፣

፲፬/ የሳይበር ክስተት ማጋጠሙን እንዳወቀ በ፵፰ ሰዓታት ውስጥ ለብሔራዊ ደንገተኛ የኮምፒውተር ምላሽ መስጫ ማዕከል የማሳወቅ፤ እና የሚሰጠውን አስገዳጅ ምክረ ሃሳቦች ወይም አቅጣጫዎችን በሚሰጠው የጊዜ ገደብ ውስጥ የመተግበር፤

፲፭/ አስተዳደሩ በሚዘረጋው ስርዓት መሰረት በየወቅቱ አስፈላጊ ኢንፎርሜሽኖችን የመለዋወጥ፤

10/ To employ cybersecurity professionals who have obtained professional certificates issued by the Administration or recognized by the Administration; to ensure that existing professionals obtain professional certification in accordance with the system established by the Administration;

11/ To ensure the security of the supply chain of the technology products used;

12/ Prior to integration, obtaining security clearance for new or upgraded information and communication technology systems acquired through purchase, donation, development, or any other means, in accordance with the system established by the Administration;

13/ Establish and manage a Center responsible for monitoring, reporting, and responding to cyber attacks in accordance with the framework to be developed by the Administration;

14/ To notify cybersecurity incidents the National Computer Emergency Response Center within 48 hours in accordance with the system established by the Administration and implement the solutions and directions to be provided;

15/ To exchange important information periodically using the information exchange system established by the Administration;

፲፮/ የሳይበር ደህንነት ልምምድና ስልጠና ፕሮግራሞችን የማዘጋጀትና የመተግበር እንዲሁም አስተዳደሩ በሚያመቻቻቸው ልምምድና ስልጠናዎች ላይ የመሳተፍ፤

፲፯/ የቁልፍ መሠረተ ልማቱ ሀብቶች ተደራሽ የሚሆኑላቸው ሠራተኞችን ወይም ኃላፊዎች በሚመለከተው የመንግሥት አካል የደህንነት ማረጋገጫ እንዲያገኙ የማድረግ፤

፲፰/ የሳይበር ደህንነት የሚጠይቀውን የሙያ ስነ ምግባር መከበሩን የማረጋገጥ።

፰. ውክልና ስለመስጠት

፩/ የቁልፍ መሰረተ ልማት ባለቤቶች በዚህ አዋጅ አንቀፅ ፯ የተደነገጉ ግዴታዎች እንደአግባብነቱ በራስ አቅም ወይም በዚህ አዋጅ መሠረት ፈቃድ በተሰጠው የሳይበር ደህንነት አገልግሎት አቅራቢ ሰው ውክልና በመስጠት ተግባራዊ ሊያደርግ ይችላል።

፪/ የዚህ አንቀፅ ንዑስ አንቀፅ (፩) ቢኖርም አስተዳደሩ ከብሔራዊ ደህንነትና ጥቅም አንፃር በውክልና የሳይበር ደህንነት አገልግሎት የማይሰጥባቸውን የቁልፍ መሰረተ ልማቶች በመመሪያ ይለያል።

፱. የአስተዳደሩ ተግባርና ኃላፊነት

አስተዳደሩ ከቁልፍ መሰረተ ልማት የሳይበር ደህንነት ከመጠበቅ አንፃር የሚከተሉት ተግባርና ኃላፊነቶች ይኖሩታል፡-

፩/ ሳይበር ደህንነት አስተዳደር ጉዳይን በተመለከተ፡-

16/ To develop and implement cybersecurity exercise and training and to participate in cyber drills and training facilitated by the Administration;

17/ To ensure that employees and officers with access to critical resources are provided with security clearance by the relevant Government body;

18/ To ensure compliance with the professional ethics required by cybersecurity.

8. Delegation

1/ The owners of critical infrastructure may implement the obligations imposed by Article 7 of this Proclamation in their capacity or by delegating to persons providing cybersecurity services licensed in accordance with this Proclamation.

2/ Notwithstanding Sub-Article (1) of this Article, the Administration shall identify critical infrastructure which cybersecurity service shall not be provided by delegation on the terms national security and interests.

9. Role and Responsibility of the Administration

The Administration shall have the following role and responsiblites related to critical infrastructure protection:

1/ Regarding Cybersecurity Management:

ሀ) አስገዳጅ ሀገራዊ የሳይበር ደህንነት ፕሮግራሞችን ይቀርጻል፤ አፈፀማቸውን ይከታተላል፤

ለ) ቁልፍ መሰረተ ልማቶች የሚያወጧቸው የሳይበር ደህንነት ፕሮግራሞች፣ ሀገራዊ የሳይበር ደህንነት ማዕቀፍን ተከትለው መዘጋጀታቸውንና መተግበራቸውን ይከታተላል፣ ይደግፋል፤

ሐ) ሀገራዊ የሳይበር ደህንነት ማዕቀፍ ትግበራ ሂደትን ይከታተላል፤ ያስፈፅማል፤

መ) ሀገራዊ የሳይበር ደህንነት አደጋ እና የደህንነት ቁመና ደረጃ ዳሰሳ ሪፖርት በየዓመቱ ያዘጋጃል፤

ሠ) ከተለያዩ ባለድርሻ አካላት ጋር በመተባበር የሳይበር ደህንነት ልምምዶችን፣ ስልጠናዎችን እና የአቅም ግንባታ ፕሮግራሞችን ያዘጋጃል ይተገብራል፤

ረ) በቁልፍ መሰረተ ልማቶች ደህንነትና አይበገሬነት ለመፍጠር የሚያስችል ሀገራዊ የሳይበር ደህንነት ፎረም ይመሰርታል፤ ያስተዳድራል፤

ሰ) የሚያወጣቸውን የሳይበር ደህንነት ማዕቀፎችን፣ የአሰራር ስርዓቶች፣ አስፈላጊ መረጃዎችን የተለያዩ ዘዴዎችን በመጠቀም ተደራሽ ያደርጋል።

a) formulates mandatory cybersecurity programs and meets the necessary organization, budget, and manpower to implement the program;

b) monitors and supports the development and implementation of cybersecurity programs by critical infrastructure organizations;

c) monitors and implements the implementation process of the National Cybersecurity Framework;

d) prepares a national cybersecurity risk, maturity, and security assessment report annually;

e) develop and implement cybersecurity drills and training in collaboration with various stakeholders;

f) establishes and administers a National Cybersecurity Forum to enforce security and resilience in critical infrastructure;

g) provides access to cybersecurity frameworks, procedures, and important information using a variety of methods.

፪/ ስለሳይበር ክስተቶች ምላሽ አሰጣጥ በተመለከተ፦

ሀ) በቁልፍ መሰረተ ልማቶች ላይ ጥቃቶች እንዳይደርሱ ተገቢውን የቅድመ መከላከል እና ጥቃቶች ሲደርሱ ምላሽ የሚሰጥበትን ስርዓት ይዘረጋል፤

ለ) አስፈላጊ ሆኖ ሲገኝ በቁልፍ መሰረተ ልማቶች ላይ የሳይበር ጥቃቶች ለመከላከል ተገቢውን ክትትልና ቁጥጥር ያደርጋል፤

ሐ) በቁልፍ መሰረተ ልማቶች ላይ የሚደርሱ የሳይበር ክስተቶች የመረጃ ልውውጥ ስርዓት ይዘረጋል፤ ለቁልፍ መሰረተ ልማቶች የቅድመ ማስጠንቀቂያ ይሰጣል፤

መ) የሳይበር ክስተቶችን በመከላከል ዙሪያ ሀገር አቀፍ፣ ቀጠናዊ፣ አህጉራዊ ወይም ዓለምአቀፋዊ የትብብርና የትስስር ግንኙነቶችን ያስተባብራል በበላይነት ይመራል፤

ሠ) በቁልፍ መሰረተ ልማት የሳይበር ክስተት ክትትል ሪፖርት እና ምላሽ እንዲሰጡ የሚቋቋሙ አደረጃጀቶች የዘረጓቸውን የአሰራር ስርዓቶች እና አፈፃፀማቸውን ይከታተላል፤ ይቆጣጠራል፤ ቅንጅታዊ አሰራር ስርዓት በመመሪያ ይዘረጋል፤

ረ) ሀገራዊ የሳይበር ጥቃት ተጋላጭነቶችን፣ የመከላከያ እርምጃዎችን እና ወቅታዊ የደህንነት ሁኔታ ሪፖርቶችን ለህዝብ በየወቅቱ ይፋ ያደርጋል፤ ተገቢውን የግንዛቤ ማስጨበጫ ስራ ይሰራል።

2/ Regarding cyber incidents response:

a) Establishes a system for appropriate preemptive defense against attacks on critical infrastructure and how to respond in the event of attacks;

b) When necessary, implement necessary monitoring and control measures to prevent cyber attacks against critical infrastructure;

c) Establish the exchange of information platform and provide early warning of cyber incidents for critical infrastructure;

d) Coordinates and oversees national, regional, continental, or international cooperation and connectivity relations in the area of prevention of cyber incidents;

e) Monitor and supervise the procedures and implementations of organizations established to monitor, report, and respond to cyber incidents in critical infrastructure; and issue Directive to establish a coordinated system of procedures;

f) Periodically disclose national cyber attack vulnerabilities, preventive measures, and timely security status reports to the public, and conduct appropriate awareness raising activities.

፫/ የሳይበር ደህንነት ኦዲትና የሳይበር ደህንነት ፍተሻና ግምገማ በተመለከተ፦

ሀ) ሀገራዊ የሳይበር ደህንነት ማዕቀፎችን መሠረት በማድረግ ቁልፍ መሠረተ ልማቶችን ቢያንስ በየዓመቱ መደበኛ እና በማንኛውም ጊዜ ድንገተኛ የሳይበር ደህንነት ኦዲት ሊያደርግ ይችላል፤ ተፈላጊ መስፈርቶቹን ለሚያሟሉ የሳይበር ደህንነት ማረጋገጫ ሰርተፍኬት ይሰጣል፤

ለ) ሀገራዊ የሳይበር ደህንነት ማዕቀፎችን እና ዓለም አቀፍ ስታንዳርዶችን መሠረት በማድረግ ቁልፍ መሠረተ ልማቶች የሳይበር ደህንነት ፍተሻና ግምገማ ያደርጋል፤ ፈቃድ ይሰጣል፤

ሐ) በዚህ አንቀፅ ንዑስ (፩) እና (፪) መሠረት የሚደረጉ የሳይበር ደህንነት ኦዲት እና የሳይበር ደህንነት ፍተሻና ግምገማዎችን በውክልና እንዲያደርጉ ለግል አገልግሎት ሰጪዎች ፈቃድ ይሰጣል፤

መ) የሳይበር ደህንነት ኦዲት እና የሳይበር ደህንነት ፍተሻና ግምገማ ማረጋገጫ ሰርተፍኬት ይሰጣል፤ ሰርተፍኬቱ ስለሚሰጥበት እና እድሳት ስለሚደረግበት አግባብ በመመሪያ ይወስናል።

፲. ስለ አገልግሎት ክፍያ

አስተዳደሩ በዚህ አዋጅ መሰረት ለሚሰጣቸው አገልግሎቶች በሚኒስትሮች ምክር ቤት በሚወጣ ደንብ መሰረት ክፍያዎችን ይሰበስባል።

3/ Regarding Cyber Security Audit and Cyber Security Inspection and Evaluation:

a) Conducts annual or ad hoc cybersecurity audits of critical infrastructure in accordance with national cybersecurity frameworks and issues cybersecurity certification certificates to those who meet the required standards;

b) Conducts and authorizes cybersecurity inspections and evaluations of critical infrastructures in accordance with national cybersecurity frameworks and International standards;

c) Authorize private service providers to conduct cybersecurity audits and cybersecurity inspections and evaluations conducted pursuant to Sub-Article (1) and (2) of this Article;

d) Issue a certificate of cybersecurity audit and cybersecurity inspection and evaluation based on the appropriate renewal and issue of the certification to be determined by Directive of the Administration.

10. Service Fee

The Administration shall collect fees for services rendered pursuant to this Proclamation through Regulation issued by Councl of Ministers.

ክፍል ሦስት

ስለፈንድ መቋቋም

፲፩. መቋቋም

፩/ የቁልፍ መሰረተ ልማቶችን ደህንነት ለማስጠበቅ የሚዘረጉ የሳይበር ደህንነት ፕሮግራሞችን እና የሳይበር ደህንነት ማዕቀፎችን ለማስተግበር የሚያስችል የቁልፍ መሰረተ ልማቶች የሳይበር ደህንነት ፈንድ በዚህ አዋጅ ተቋቁሟል፡፡

፪/ ፈንዱ ቋሚ የፋይናንስ ምንጭ ሆኖ ለፈንዱ ዓላማ ማስፈፀሚያ ይውላል፡፡

፲፪. የፈንዱ ዓላማዎች

ፈንዱ የሚከተሉት ዓላማዎች ይኖሩታል፡-

፩/ የቁልፍ መሰረተ ልማቶችን ደህንነት ለማስጠበቅ በአስተዳደሩ የሚዘጋጁ የሳይበር ደህንነት ፕሮግራሞችን እና የሳይበር ደህንነት ማዕቀፎችን ለማስተገበር የሚያስችል ድጋፍ ለማድረግ፤

፪/ የቁልፍ መሰረተ ልማቶችን ደህንነትን ለማስጠበቅ የሚደረጉ የጥናትና ምርምር ተግባራትን መደገፍ፤

፫/ የቁልፍ መሰረተ ልማት ተቋማትን አቅም ለመገንባት የሚያስችሉ ሀገር አቀፍ እና ዓለም አቀፍ የስልጠና፣ ልምምድ እና የአቅም ግንባታ ፕሮግራሞችን ለመደገፍ፤

፬/ ቁልፍ መሠረተ ልማቶችን ደህንነት ለማስጠበቅ ለሚፈፀሙ ተግባራት እና ሥራውን በቴክኖሎጂ የተደገፈ ለማድረግ የሚያግዙ አስቻይ መሰረተ ልማቶችንና ስርዓቶችን ለማሟላት፤

PART THREE

FUND ESTABLISHEMENT

11. Establishment of the Fund

1/ A Critical Infrastructure Cyber Security Fund is hereby established by this Proclamation to implement cyber security programs and frameworks designed to safeguard the security of key infrastructures.

2/ The Fund shall be a permanent source of financing and shall be used for the implementation of the objectives of the Fund.

12. Objectives of the Fund

The Fund shall have the following objectives:

1/ To support the implementation of cybersecurity programs and cybersecurity frameworks developed by the Administration to protect the security of critical infrastructures;

2/ To support research and development activities aimed at the protection of critical infrastructures security;

3/ To support National and International training, drills and capacity building programs to build the capacity of critical infrastructure institutions;

4/ To provide enabling infrastructures and platforms for the activities carried out to protect the security of critical infrastructure and to enable the work to be supported by technology;

፭/ ለዜጎች የሳይበር ደህንት ግንዛቤ ለመፍጠር ለሚከናወኑ ሀገራዊ ንቅናቄዎችና ኩነቶችን ለመደገፍ፤

፮/ የቁልፍ መሠረት ልማቶችን የሳይበር ደህንነት ለማስጠበቅ በግለሰቦች፣ በቡድኖች ወይም በማህበረሰቦች ተነሳሽነትና በጎ ፈቃደኝነት የሚከናወኑ ሥራዎችን በተቀናጀ ለመደገፍና ለማስተባበር።

፲፫. <u>የፈንዱ ምንጭ</u>

፩/ የፈንዱ ምንጮች የሚከተሉት ናቸው፡-

ሀ) ቁልፍ መሰረተ ልማቶች በሚኒስትሮች ምክር ቤት በሚወጣ ደንብ ተወስኖ የሚያዋጡት መዋጮ፤

ለ) ከገቢ ማሰባሰቢያ ፕሮግራሞች በፈቃደኛነት ከተቋማት እንዲሁም ግለሰቦች የሚገኙ ድጋፎች፤

ሐ) ከአገልግሎት ክፍያዎችና ከአስተዳደራዊ ቅጣት የሚሰበሰቡ ገቢዎች፤

፪/ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሠረት የተገኘው ገንዘብ ለፈንዱ ተብሎ በገንዘብ ሚኒስቴር በተከፈተ የባንክ ሂሳብ ተቀማጭ ይደረጋል።

፲፬. <u>የፈንዱ ተሰብሳቢ ገቢ</u>

፩/ በዚህ አዋጅ አንቀፅ ፲፫ ንዑስ አንቀፅ (፩) መሠረት የሚሰበሰቡ ገቢዎች በየወሩ መጨረሻ በአስተዳደሩ እየተሰበሰቡ ለፈንዱ ገቢ ይሆናሉ፤

5/ To support national campaigns and events organized to enhance cyber security awareness among citizens

6/ To support and coordinate the initiatives and voluntary work undertaken by individuals, groups, or communities to ensure the cybersecurity of critical infrastructure developments.

13. <u>Source of Funds</u>

1/ The sources of funds are as follows:

a) Contributions from critical infrastructures determined by a Regulation issued by the Council of Ministers;

b) Support obtained voluntarily from institutions and individuals through fund raising programs;

c) Revenues collected from service fees and administrative fines pursuant to this Proclamation;

2/ The funds obtained pursuant to Sub-Article (1) of this Article shall be deposited in a bank account opened by the Ministry of Finance for the purpose of the Fund;

14. <u>Collection of Fund</u>

1/ The revenues collected in accordance with Article 13, Sub-Article (1) of this Proclamation shall be collected by the Administration at the end of each month and shall be deposited in the account of the Fund;

፪/ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሠረት አስተዳደሩ ገቢ ማድረጉን በ፯ /ሰባት/ ተከታታይ ቀናት ውስጥ ለገንዘብ ሚኒስቴር ያሳውቃል፡፡

፲፭. <u>ስለፈንዱ አስተዳደርና አጠቃቀም</u>

የፈንዱ አስተዳደር፣ አጠቃቀም እና ዝርዝር የአሰራር ስርዓት በሚኒስትሮች ምክር ቤት በሚወጣ ደንብ ይወሰናል።

ክፍል አራት
ስለሳይበር ደህንነት አገልግሎት ሰጪዎች

፲፮. <u>ለሳይበር ደህንነት አገልግሎት ሰጪዎች ፈቃድ</u>

፩/ አስተዳደሩ የሳይበር ደህንነት አገልግሎትን ለመስጠት የሚያስችል ፈቃድ ይሰጣል፤

፪/ ማንኛውም ሰው በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሠረት በአስተዳደሩ የሚሰጠው ፈቃድ ሳይኖረው የሳይበር ደህንነት ምርት ወይም አገልግሎቶችን መስጠት አይችልም፤

፫/ አስተዳደሩ ፈቃድ የሚያስፈልጋቸውን የሳይበር ደህንነት ምርትና አገልግሎት ዓይነቶችን፣ ፈቃድ ለማግኘት ስለሚቀርብ ማመልከቻ ሥርዓት፣ ስለፈቃድ ይዘት፣ ምላሽ ስለሚሰጥበት፣ ፍቃድ ስለሚታደስበት፣ ክትትልና ቁጥጥር ስለሚደረግበት፣ የደህንነት ማረጋገጫ ሰለሚሰጥበት፣ ቅሬታ ስለሚቀርብበት እና ሌሎች አግባብነት ያላቸው ጉዳዮች አስመልክቶ ዝርዝሩን በመመሪያ ይወስናል።

2/ The Administration shall notify the Ministry of Finance within 7 /Seven/ days of the receipt of revenue in accordance with Sub-Article (1) of this Article.

15. <u>Administration and Utilization of the Fund</u>

The administration, utilization, and detailed operational procedures of the Fund shall be determined by a Regulation to be issued by the Council of Ministers.

PART FOUR
CYBERSECURITY SERVICE PROVIDERS

16. <u>Authorization for Cybersecurity Product and Service providers</u>

1/ The Administration shall issue a license pursuant to this Proclamation for the provision of cybersecurity products and services;

2/ Provision of cybersecurity product and service without a licende issued as per Sub-Article (1) of this Ariticle is prohibited;

3/ The Administration by issuing a Directive shall determine the types of cybersecurity products and services that require a license, the application system for licensing, the content of the licence, the response process, the control and followup, the issuance of security clearance, the filing of complaints, and other relevant matters.

፲፯. ፈቃድ የሚሰጥባቸው ዋና መስፈርቶች

በዚህ አዋጅ አንቀፅ ፲፮ መሠረት ፈቃድ ለማግኘት የሚያመለክት ሰው የሚከተሉትን ቅድመ ሁኔታዎች ማሟላት ይኖርበታል፡-

፩/ የሕግ ሰውነት ማረጋገጫ ወይም መቋቋሚያ ሰነድ፤

፪/ ተገቢውን የደህንነት ማረጋገጫ ያገኘ፤

፫/ ዝርዝሩ በመመሪያ የሚወሰን ሆኖ አገልግሎቱን ለመስጠት የሚያስችል ባለሙያዎች፣ ቴክኖሎጂ፣ የአሰራር ስርዓት ማሟላት፤

፬/ ዝርዝሩ በመመሪያ የሚሰወሰን ሆኖ አገልግሎቱን ለመስጠት የሚያስችል ካፒታል እና ተመጣጣኝ ዋስትና፤

፭/ በኢትዮጵያ ቋሚ አድራሻ፤

፮/ በፍርድ ወይም በሕግ ችሎታውን ያላጣ፤

፯/ በማጭበርበር፣ ሙስና ወይም ከእምነት ማጉደል ጋር ተያያዥ በሆኑ ወንጀሎች ተፈርዶበት የማያውቅ፤ ወይም የተሰየመ፤ እና

፰/ ፈቃድ እንደሚሰጥበት የሳይበር ደህንነት አገልግሎት አስተዳደሩ በመመሪያ የሚያወጣቸው ዝርዝር መስፈርቶችን።

፲፰. ፈቃድ የተሰጠው ሰው ግዴታ

በዚህ አዋጅ መሠረት ፈቃድ የተሰጠው ማንኛዉም ሰው የሚከተሉት ግዴታዎች ይኖሩታል፡-

17. Requirements for licensing

A person applying for a license under Article 16 of this Proclamation must meet the following conditions:

1/ Legal entity certificate or establishment document;

2/ Attain appropriate security clearance;

3/ Meet the requirements for professionals, technology, and operational systems necessary to provide the service, the details of which shall be determined by a Directive;

4/ Possess the minimum capital and provide a commensurate guarantee necessary to provide the service, the details of which shall be determined by a Directive;

5/ a permanent address in Ethiopia;

6/ has not lost all or part of his capacity in judgment or law;

7/ Has never been convicted of crimes related to fraud, corruption or breach of trust; and

8/ Detailed requirements of the Cybersecurity Service for which a license is issued shall be determined by Directive to be issued by the Administration.

18. Duty of a licensed person

Any person licensed pursuant to this Proclamation shall have the following obligations:

፩/ የተሰጠውን ፈቃድ ለተፈቀደለት ዓላማ እና ወሰን ብቻ የመጠቀም፤

፪/ የተሰጠዉን ፍቃድ ለሦስተኛ ወገን በማናቸውም መልኩ አስተዳደሩን ሳያሳውቅና ፈቃድ ሳያገኝ ያለማስተላለፍ፣ ያለማዋስ፣ እንዲጠቀምበት ያለማድረግ፤

፫/ ለፈቃዱ መሰጠት አስፈላጊ የሆኑ መስፈርቶች ላይ ለውጥ ሲኖር ለአስተዳደሩ ወዲያውኑ የማሳወቅ፤

፬/ በስራ አጋጣሚ ያገኛቸውን መረጃዎች በሚስጥር የመያዝ፤

፭/ አስተዳደሩ የቁጥጥር ኃላፊነቱን በሚወጣበት ወቅት የሚጠይቃቸውን አስፈላጊ መረጃዎች የማቅረብና ለሚያነሳቸው ጥያቄዎች ተገቢውን ትብብር የማድረግ፤ እና

፮/ ይህን አዋጅ እና አዋጁን ለማስፈፀም የሚወጡ ደንቦች እና መመሪያዎች ላይ የተቀመጡ ሌሎች ግዴታዎች ማክበር።

፲፱. ፈቃድ ስለመሰረዝ

በዚህ አዋጅ መሠረት የተሰጠ ፈቃድ ከሚከተሉት ሁኔታዎች በአንዱ ሊሰረዝ ይችላል፡-

፩/ ፈቃዱን ለማግኘት የቀረቡ መረጃዎች የተጭበረበሩ ወይም ሀሰተኛ ሆነው ሲገኙ፤

፪/ የተሰጠውን ፈቃድ ከተሰጠው ዓላማና ወሰን ውጪ ጥቅም ላይ እየዋለ መሆኑ ሲረጋገጥ፤

1/ To use the license granted only for the purpose and scope for which it is authorized;

2/ Not to transfer, lend, or allow a third party to use the license granted in any manner without notifying or obtaining permission from the Administration;

3/ To notify the Administration immediately when there is a change in the requirements for the issuance of the license;

4/ To keep confidential information obtained in the course of his duty;

5/ To provide the necessary information requested by the Administration in the discharge of its supervisory responsibilities and to respond appropriately to the questions raised; and

6/ comply with this Proclamation and other obligations set out in the Regulations and Directives for the implementation of the Proclamation.

19. Revocation of licenses

The Administration shall revoke the license if one of the following conditions are met:

1/ the information provided for the purpose of obtaining the license is found to be fraudulent or falsified;

2/ where it is determined that the license is being used outside the objective and scope for which it was granted;

፫/ ፈቃድ የተሰጠው ሰው ይህን አዋጅ እና አዋጁን ለማስፈፀም የሚወጡ ደንብና መመሪያዎች ላይ የተደነገጉ ስርዓቶች ላይ ጥሰቶችን መፈፀሙ ሲረጋገጥ፤

፬/ የተሰጠው ፈቃድ የጊዜ ገደብ ሲያበቃ እና ሳይታደስ ሲቀር፤

፭/ ፈቃድ የተሰጠው ሰው ሲሞት ወይም በሕግ ወይም በፍርድ ችሎታውን ሲያጣ፤ ወይም ፈቃድ የተሰጠው ድርጅት ሲፈርስ፣ በህግ መክሰሩ ሲረጋገጥ ወይም ሲዘጋ፤

፮/ ፍቃድ የተሰጠው ሰው በማጭበርበር፣ በማታለል ወይም እምነት በማጉደል ወንጀል ተከሶ የተፈረደበት ከሆነ፤

፯/ ፈቃዱን ለማግኘት ከሚያስፈልጉ መስፈርቶች ውስጥ አንዱ ሲጓደል፤ወይም

፰/ ባለፈቃዱ አገልግሎት መስጠቱን ሲያቋርጥ እና ፈቃዱን ሲመልስ።

፳. ፈቃድ ስለማገድ

፩/ አስተዳደሩ በዚህ አዋጅ አንቀፅ ፲፱ የተዘረዘሩት ሁኔታዎች ስለመኖራቸው አሳማኝ ሁኔታ በሚኖርበት ወቅት ጉዳዩ እስኪጣራና እስኪረጋገጥ አስፈላጊ ሆኖ ከተገኘ ፈቃዱ እስከ ስልሳ ተከታታይ ቀናት ድረስ እንዲታገድ ሊወስን ይችላል።

፪/ አስተዳደሩ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሰረት በሚያደርገው ማጣራት የተጠረጠሩ ጥፋቶች መፈፀማቸውን ካረጋገጠ ፈቃዱን ይሰርዛል፤ ወይም እንደ ጥፋቱ ክብደት በማስጠንቀቂያ ሊያልፍ ይችላል፤ ጥፋቱን መፈፀሙ ካልተረጋገጠ ባለፈቃዱ ስራውን እንዲጀምር ይፈቀዳል።

3/ when the licensed person is found to have violated the Directives and Regulations issued for the implementation of this Proclamation and the Proclamation;

4/ when the license granted expires and is not renewed;

5/ when the licensed person dies or loses his capacity by law or judgment, or when the licensed Organization is dissolved, declared bankruptcy by law, or closed;

6/ If the licensed person has been convicted of fraud, deception, and breach of trust;

7/ when one of the requirements for obtaining the license is not met; or

8/ When the licensee ceases to provide service.

20. Suspension of License

1/ Where there is a reasonable ground to believe that the conditions specified under Article 19 of this Proclamation exist, the Administration may, if it deems it necessary until the matter investigated and verified, suspend the license for a period of up to Sixty consecutive days.

2/ If the Administration confirms, in the course of its investigation pursuant to Sub Article (1) of this Article, that the suspected offenses have been committed, it shall revoke the license; or if the offense is found to be minor, it may be dismissed with a warning.

፳፩. ለባለሙያዎች የሙያ ማረጋገጫ ወይም እውቅና መስጠት

አስተዳደሩ በቁልፍ መሰረተ ልማቶች ውስጥ የሳይበር ደህንነት ተግባር ለሚያከናውኑ የሳይበር ደህንነት ባለሙያዎች የሙያ ማረጋገጫ ወይም እውቅና ምስክር ወረቀት የሚሰጥበት ስርዓት በመመሪያ ይዘረጋል።

ክፍል አምስት

ስለአስተዳደራዊ እርምጃ እና ቅሬታ አቀራረብ ስርዓት

፳፪. አስተዳደራዊ እርምጃ

፩/ ማንኛውም የቁልፍ መሰረተ ልማት ባለቤት በዚህ አዋጅና አዋጁን ለማስፈፀም የሚወጡ ደንብና መመሪያ በመጣስ ሆን ብሎ፦

ሀ) አስገዳጅ የሳይበር ደህንነት ማዕቀፎችን በወቅቱ ካልተገበረ ከአምስት መቶ ሺህ እስከ አንድ ሚሊዮን ብር፤

ለ) የሚያጋጥሙ የሳይበር ደህንነት ክስተቶችን ለብሔራዊ ድንገተኛ የኮምፒውተር አደጋ ምላሽ መስጫ ማዕከል በ፵፰ ሰዓታት ውስጥ ካላሳወቀ ወይም ተገቢውን የእርምት እርምጃ ሳይወስድ ከቀረ ከአንድ ሚሊዮን አምስት መቶ ሺህ እስከ ሁለት ሚሊዮን ብር፤

21. Accreditation for professionals

The Administration by issuing a Directive shall establish a system for the issuance of professional certifications or accreditations to cybersecurity professionals performing cybersecurity functions within critical infrastructure.

PART FIVE

ADMINISTRATIVE MEASURES AND COMPLIANT PROCEDURE

22. Administrative Measures

1/ Any owner of a critical infrastructure who intentionally violates any Directive or Regulations issued for the implementation of this Proclamation or the Proclamation shall be subject to an administrative penalty:

a) Does not implement mandatory cybersecurity framework in a timely manner: shall be fined from Five Hundred Thousand to One Million Birr;

b) If it fails to notify cybersecurity incidents the National Emergency Computer Incident Response Center with in 48 hours or fails to take appropriate corrective action shall be fined from One Million Five Hundred Thousand to Two Million Birr;

ሐ) ብሔራዊ ድንገተኛ የኮምፒውተር አደጋ ምላሽ መስጫ ማዕከል ለሳይበር ጥቃቶች ምላሽ ለመስጠት በሚያደርገው እንቅስቃሴ አስፈላጊ መረጃዎችን ካልሰጠ ወይም ተገቢውን ትብብር ካላደረገ ከሦስት መቶ ሺህ እስከ አምስት መቶ ሺህ ብር፤

መ) በየጊዜው ለሚደረገው የሳይበር ደህንነት ኦዲት ተገቢውን ትብብር ካላደረገ፤ ከአንድ ሚሊዩን አምስት መቶ ሺህ እስከ ሁለት ሚሊዮን፤

ሠ) በሳይበር ኦዲት የተገኙ ክፍተቶች ላይ አስተዳደሩ ማስተካከያ እንዲያደርግ በተሰጠው አቅጣጫ መሠረት ተገቢውን የእርምት እርምጃ በወቅቱ ካልወሰደ ከስምንት መቶ ሺህ እስከ አንድ ሚሊዮን ብር፤

ረ) የሳይበር ደህንነት ፍተሻና ግምገማ ያልተደረገባቸውን የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ስርዓቶችን በማናቸውም መልኩ ከተጠቀመ፤ ከስምንት መቶ ሺህ ብር እስከ አንድ ሚሊየን ብር፤

አስተዳደራዊ መቀጮ ይቀጣል።

፪/ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) የተደነገጉ ጥፋቶች በቸልተኝነት የተፈፀሙ ከሆነ እንደ ጥፋቱ ዓይነት በንዑስ አንቀፁ ከተደነገጉ አስተዳደራዊ የገንዘብ መቀጮዎች ከግማሽ ባልበለጠ ይቀጣል።

c) If it fails to provide necessary information or cooperate appropriately with the National Emergency Computer Incident Response Center in its activities in responding to cyberattacks; shall be punished from Three Hundred Thousand to Half a Million Birr;

d) Fails to cooperate appropriately with periodic cybersecurity audits; shall be fined from One Million Five Hundred Thousand to Two Million;

e) Failure to implement timely corrective action, as directed by the Administration to correct the gaps identified in cyber audit shall result in a fine of Eight Hundred Thousand to One Million Birr;

f) The use of information communication technology systems in any manner that has not been subject to cybersecurity inspection and evaluation; shall be fined from Eight Hundred Thousand to One Million Birr;

2/ If the offenses provided for in Sub-Article (1) of this Article are committed through negligence, the applicable administrative fines prescribed therein shall be reduced by no less than (1/2) one-half.

፫/ በዚህ አንቀፅ ንዑስ (፩) እና (፪) የተደነገገው ቢኖርም ጥፋቱ የተፈፀመው ለመጀመሪያ ጊዜ ከሆነ እና ምንም አይነት ጉዳት ያልደረሰ ከሆነ አስተዳደሩ ተገቢው የእርምት እርምጃ እንዲወሰድ የጽሁፍ ማስጠንቀቂያ ብቻ በመስጠት ያልፈዋል፤

፬/ ማንኛውም ሰው በዚህ አዋጅ አንቀፅ ፲፮ ንዑስ አንቀፅ (፪) በመተላለፍ የፀና ፈቃድ ሳይኖረው የሳይበር ደህንነት አገልግሎት የሰጠ እንደሆነ ወይም በአንቀፅ ፲፰ የተደነገጉ ግዴታዎችን ተላልፎ ከተገኘ ከብር አንድ ሚሊዮን ሁለት መቶ ሺህ ብር እስከ ሁለት ሚሊዮን ብር ይቀጣል፤

፭/ በዚህ አንቀፅ የተዘረዘሩ ጥፋቶችን የቁልፍ መሰረተ ልማት ባለቤቱ ወይም የሳይበር ደህንነት አገልግሎት የሚሰጥ አካል ከአንድ ጊዜ በላይ የፈጸመ እንደሆነ ለጥፋቱ የተጠቀሰውን ትልቁን የገንዘብ መጠን በሶስት እጥፍ እንዲከፍል ይደረጋል፤

፮/ አስተዳደሩ በዚህ አንቀፅ መሠረት የሚጣሉ አስተዳደራዊ ቅጣቶችን ያስፈፅማል፤

፯/ በዚህ አንቀፅ ስር የተመላከቱ የአስተዳደራዊ የገንዘብ ቅጣቶች እንደ አስፈላጊነቱ በሚኒስትሮች ምክር ቤት በሚወጣ ደንብ ሊሻሻሉ ይችላሉ።

3/ Notwithstanding the provisions of Sub-Article (1) and (2) of this Article, if the offense is committed for the first time and no damage has occurred, the Administration may waive it by issuing a written warning to take appropriate corrective action;

4/ Any person who provides cybersecurity services without a valid license in violation of Sub-Article (2) of Article 16 of this Proclamation, or if a licensed person is found to have violated the obligations set out in Article 18 of this Proclamation, shall be fined from One Million Two Hundred Thousand to Two Million Birr;

5/ Where a critical infrastructure owner or a cybersecurity service provider commits the offenses specified under this Article more than once, they shall be punished with a fine equivalent to triple the maximum amount prescribed for the offense;

6/ The Administration shall enforce administrative penalties imposed pursuant to this Article;

7/ The administrative financial penalties specified under this Article may be revised by a Regulation to be issued by the Council of Ministers, as may be necessary.

፳፫. የቅሬታ አፈታት

፩/ ማንኛውም ቁልፍ መሰረተ ልማት ወይም ሰው ከዚህ አዋጅ እና አዋጁን ተከትለው ከሚወጡ ደንብ፣ መመሪያ ወይም ስታንዳርዶች አፈፃፀም ጋር በተያያዘ ለሚኖረው ማንኛውም አይነት ቅሬታ የቅሬታው መንስዔ ከታወቀበት በኋላ ባሉት ተከታታይ ፴ ቀናት ውስጥ አቤቱታውን ለአስተዳደሩ በፅሑፍ ማቅረብ ይኖርበታል።

፪/ አስተዳደሩ በዚህ አንቀፅ ንዑስ አንቀፅ (፩) መሠረት የቀረበለትን አቤቱታ ከቀረበለት በ፲፭ ተከታታይ የስራ ቀናት ውስጥ አስፈላጊውን ውሳኔ መስጠት ይኖርበታል፤ ዝርዝር የቅሬታ አቀራረብ ስርዓቱ በአስተዳደሩ በሚያወጣው መመሪያ ይወሰናል።

፫/ አስተዳደሩ በሰጠው ውሳኔ ላይ የሚቀርቡ ቅሬታዎችን የሚያስተናግድ ከሚመለከታቸው የመንግስት እና የግል ዘርፍ አካላት የተውጣጣ ቦርድ በደንብ ይቋቋማል፤ ቦርዱ ቅሬታ የሚያስተናግድበት ስርዓት በደንብ ይወሰናል።

፬/ ቦርዱ በሰጠው ውሳኔ ያልረካ ማንኛውም ሰው ይግባኙን በ፷ ቀናት ውስጥ አግባብነት ላለው ፍርድ ቤት ሊያቀርብ ይችላል።

23. Complaint Handling

1/ Any critical infrastructure or person shall submit a written complaint to the Administration within 30 consecutive days after the occurrence of the cause of the complaint in relation to the implementation of this Proclamation and the rules, Regulations or standards issued pursuant to it.

2/ The Administration shall issue the decision within 15 consecutive working days of the receipt of a complaint submitted to it under Sub-Article (1) of this Article; the detailed procedure for submitting complaints shall be determined by a Directive issued by the Administration.

3/ A Board, composed of relevant Government and Private sector stakeholders, shall be established by a Regulation to handle grievances arising from the decisions of the Administration; the procedures for grievance handling by the Board shall be determined by the Regulation.

4/ Any person aggrieved by the decision of the Board may appeal to the competent court within 60 (Sixty) consecutive days.

ክፍል ስድስት

ልዩ ልዩ ድንጋጌዎች

፳፬. የመተባበር ግዴታ

ማንኛውም ሰው አስተዳደሩ በዚህ አዋጅ የተሰጡትን ኃላፊነቶች ለመወጣት የሚወስዳቸውን እርምጃዎች የማክበርና የመተባበር ግዴታ ይኖርበታል፡፡

፳፭. የወንጀል ተጠያቂነት

፩/ ማንኛውም የቁልፍ መሠረተ ልማት የሳይበር ደህንነት ኃላፊ፣ ሠራተኛ፣ የአስተዳደር አካል ወይም ባለቤት፣ ይህን አዋጅ በመጣስ ሆን ብሎ፡-

ሀ) አስገዳጅ የሳይበር ደህንነት ማዕቀፎችን በወቅቱ ካልተገበረ ወይም መተግበሩን ካላረጋገጠ፤

ለ) የሚያጋጥሙ የሳይበር ጥቃቶች ለብሔራዊ ድንገተኛ የኮምፒውተር አደጋ ምላሽ መስጫ ማዕከል በ፵፰ ሰዓታት ውስጥ ካላሳወቀ ወይም ተገቢውን የእርምት እርምጃ ሳይወስድ ከቀረ፤

ሐ) በሳይበር ኦዲት የተገኙ ክፍተቶች ላይ አስተዳደሩ ማስተካከያ እንዲያደርግ በሰጠው አቅጣጫ መሠረት ተገቢውን የእርምት እርምጃ በወቅቱ ካልወሰደ፤

መ) የሳይበር ደህንነት ፍተሻና ግምገማ ያልተደረገባቸውን የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ ስርዓቶችን በማናቸውም መልኩ ከተጠቀመ ወይም ጥቅም ላይ እንዲውሉ ካደረገ፤

PART SIX

MISCELLANEOUS PROVISIONS

24. Obligation to Cooperate

Everyone shall be obliged to comply with and cooperate with the measures taken by the Administration to fulfill the responsibilities conferred by this Proclamation.

25. Criminal Liability

1/ Any cybersecurity officer, employee, member of the management body, or owner of a critical infrastructure who, intentionally violates this Proclamation by:

a) Failure to implement or ensure the timely implementation of mandatory cybersecurity frameworks;

b) Failure to notify the National Computer Emergency Response Center of cyber attacks with in 48 hours, or failure to implement appropriate corrective actions;

c) Failure to take appropriate corrective action in a timely manner in response to the gaps identified by the Administration's cyber audit;

d) Anyone who uses or causes to be used information and communication technology systems that have not undergone cybersecurity testing and evaluation in any way is;

እስከ አንድ አመት በሚደርስ ቀላል እስራት ይቀጣል።

፪/ በዚህ አንቀጽ ንዑስ አንቀጽ (፩) ላይ የተደነገገው ወንጀል የቁልፍ መሰረተ ልማት አገልግሎትን ያቋረጠ ወይም ያስተጓጎለ ወይም ጉዳት ያደረሰ ወይም ተዓማኒነቱን ያሳጣ ወይም ሚስጥራዊነቱን ያጋለጠ ወይም በሀገር ደህንነት ወይም ጥቅም ወይም በዜጎች ጤና ወይም ህይወት ወይም በከባቢ አየር ላይ ጉዳት ያደረሰ ከሆነ ጥፋተኛው ከሰባት ዓመት እስከ አስር ዓመት በሚደርስ ፅኑ እስራት ይቀጣል።

፫/ የዚህ አንቀጽ ንዑስ አንቀጽ (፩) የተጠቀሰው የወንጀል ድርጊት በቸልተኝነት የተፈፀመ ከሆነ ቅጣቱ እንደአግባብነቱ እስከ ስድስት ወር በሚደርስ ቀላል እስራት ይሆናል።

፬/ በዚህ አንቀጽ ንዑስ አንቀጽ (፪) የተጠቀሰው የወንጀል ድርጊት የተፈፀመው በቸልተኝነት ከሆነ ቅጣቱ እንደአግባብነቱ ከሦስት እስከ አምስት ዓመት የሚደርስ ጽኑ እስራት ይሆናል።

፳፮. <u>ተፈጻሚ ስለማይሆኑ ሕጎች</u>

ከዚህ አዋጅ ጋር የሚቃረን ማንኛውም ሕግ ወይም ልማዳዊ አሠራር በዚህ አዋጅ በተሸፈኑ ጉዳዮች ላይ ተፈጻሚነት አይኖረውም።

፳፯. <u>ደንብና መመሪያ ስለማውጣት</u>

፩/ የሚኒስትሮች ምክር ቤት ይህን አዋጅ ለማስፈጸም የሚያስፈልጉ ደንቦችን ሊያወጣ ይችላል።

Punishable by up to One year in simple imprisonment.

2/ Where the offense stipulated under Sub-Article (1) of this Article results in the interruption, disruption, or damage of a critical infrastructure service; or compromises its integrity or confidentiality; or causes harm to national security, national interest, public health or life, or the environment; the offender shall be punished with rigorous imprisonment from Seven to Ten years.

3/ If the criminal act referred to in Sub-Article (1) of this Article is committed through negligence, the punishment shall be simple imprisonment for a term not exceeding Six month, as appropriate.

4/ If the criminal act referred to in Sub-Article (2) of this Article is committed through negligence, the punishment shall be rigorous imprisonment Three to Five years, as appropriate.

26. <u>Inapplicable Laws</u>

Any law or customary practice inconsistent with this Proclamation shall not apply to matters referred to in this Proclamation.

27. <u>Issuing Directive and Regulation</u>

1/ The Council of Ministers shall issue Regulations necessary for the implementation of this Proclamation.

፪/ አስተዳደሩ በዚህ አዋጅና በዚህ አንቀጽ ንዑስ አንቀጽ (፩) መሠረት የወጡ ደንቦችን ለማስፈጸም የሚያስፈልጉ መመሪያዎችን ሊያወጣ ይችላል።

፳፰. <u>አዋጁ የሚጸናበት ጊዜ</u>

ይህ አዋጅ በፌደራል ነጋሪት ጋዜጣ ታትሞ ከወጣ ከአንድ አመት በኃላ የጸና ይሆናል።

አዲስ አበባ ሐምሌ ፲፬ ቀን ፪ሺ፲፰ ዓ.ም

ታዬ አጽቀሥላሴ

የኢትዮጵያ ፌደራላዊ ዲሞክራሲያዊ ሪፐብሊክ ፕሬዚዳንት

2/ The Administration shall issue Directives for the implementation of Regulations issued pursuant to this Proclamation and Sub-Article (1) of this Article.

28.<u>Effective Date</u>

This Proclamation shall enter into force One year after its publication in the Federal Negarit Gazette.

Done at Addis Ababa, On this 21th day of July, 2026

TAYE ATSKE SELASSIE

PRESIDENT OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA