Legal Notice No ……

THE KENYA INFORMATION AND COMMUNICATIONS ACT (NO. 2 OF 1998)

THE KENYA INFORMATION AND COMMUNICATIONS (ELECTRONIC CERTIFICATION ADMINISTRATION) REGULATIONS, 2023

ARRANGEMENT OF REGULATIONS

IN EXERCISE of the powers conferred by sections 83R of the Kenya Information and Communications Act, 1998, the Cabinet Secretary of Information, Communications and Digital Economy in consultation with the Communications Authority of Kenya makes the following Regulations: -

THE KENYA INFORMATION AND COMMUNICATIONS (ELECTRONIC CERTIFICATION ADMINISTRATION) REGULATIONS, 2023

PART I - PRELIMINARIES

Short Title

1. These Regulations may be cited as the Kenya Information and Communications (Electronic Certification Administration) Regulations, 2023

Interpretation

2. In these regulations unless the context otherwise requires:-

"**Act**" means the Kenya Information and Communications Act, 1998 and any revision thereof;

"Advanced electronic signature" means an electronic signature that meets all the following requirements

a) is uniquely linked to the signatory;

b) is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it is related in such a manner that any subsequent change to the data is detectable;

"Approved digital signature scheme" means a digital signature scheme approved under regulation 8;

"Approved fee" means a fee or charge imposed to a licensed certification authority, under the Act and these Regulations that is approved by the Authority under regulation 6;

"Authority" means the Communications Authority of Kenya established pursuant to section 3 the Kenya Information and Communications Act Cap 411A;

"**Cabinet Secretary**" means the Cabinet Secretary for the time being responsible for Information, Communication and Technology

"Certificate" means a record which is issued by a certification service provider for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person

who holds a particular key pair; identifies the certification service provider issuing it; names or identifies the person to whom it is issued; contains the public key of the person to whom it is issued; and is signed by a responsible officer of the certification service provider issuing it;

"Certification practice statement" means a statement of the practices that a certification service provider employs when approving or rejecting certificate applications, or issuing, managing or revoking certificates;

"Certification service provider" means a person who has been granted a licence to issue a digital signature certificate;

"Certification personnel" means any person who has—
(a) direct responsibility for the day-to-day operations, security and performance of any activity, relating to a certification service provider, regulated under the Act and these Regulations; or
(b) duties that directly involve the issuance, renewal, suspension, revocation of certificates and creation of private keys or administration of a certification service provider's computing facilities;

"Digital certificate" is a file or electronic password that proves the authenticity of a device, or server and allows a person and/or organization to exchange data securely over the Internet using the public key infrastructure (PKI) through the use of cryptography. Digital Certificate is also known as a public key certificate or identity certificate;

"Digital signature" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine—
(a) whether the transformation was created using the private key that corresponds to the signer's public key; and
(b) whether the message has been altered since the transformation was made;

"Electronic Certification Service Provider" refers to Certification Service Provider as defined in the Act; "certification service provider" means a person who has been granted a licence to issue a digital signature certificate "Electronic Record" means a record created, generated, sent and communicated, received, or stored by electronic means;

"Electronic Signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

"Foreign Electronic Certification Service Provider" refers to a person who has been granted a licence to issue a digital signature certificate after

compliance with all the requirements for recognition under regulation 132 and has been granted recognition under regulation 164;

"Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates;

"Licensee" means a person licensed under the Act; "Licensed certification authority" means a certification authority to whom a licence has been issued by the Authority and whose licence is in effect;

"Private key" means the key of a key pair used to create a digital signature;

"Public key" means the key of a key pair used to verify a digital signature; and

"Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward;

Objects and purposes

3. The purpose of these Regulations is to provide a framework for the administration and issuance of electronic certification services.

Application

4. These Regulations shall apply to all persons involved in the provision of electronic certification services.

PART II- LICENSING OF ELECTRONIC CERTIFICATION AUTHORITIES AND PROVIDERS

Licence for Electronic Certification Services

5. The Authority may, upon application in the specified manner and subject to such requirements as it may consider necessary, grants a licence to a person to provide electronic certification services.

Operating without a Licence

6. No person shall carry on or operate, or hold himself out as carrying on or operating, as a licensed certification service provider unless that person has been issued with a licence by the Authority.

Licence requirements

7. A person applying for a licence shall, in addition to the requirements prescribed in the Act and any Regulations made thereunder —

    (a) submit for approval a certification practice statement, which fulfills the requirements prescribed in these Regulations;

(b) undergo and pass an initial audit; and fulfill other requirements relating to qualification, expertise, manpower, financial resources and infrastructure facilities necessary to issue an advanced electronic signature certificate as may be prescribed by the Authority from time to time.

Issuance of Licence

8. 1) A licence to operate as an electronic certification service provider shall be in the prescribed Form.

(2) the Authority shall specify the prescribed licensing fees and the duration of the licence.

Replacement and amendment of Licence

9. (1) A licensed certification service provider may apply to the Authority to amend-
(a) The particulars of the licence; or
(b)The issuance of a duplicate licence.

(2) An application under sub regulation (1) shall be in writing and shall be submitted to the Authority.

(3) All amendments/ replacements shall be accompanied by the prescribed fee.

(4) If the Authority approves the amendment, the Authority shall amend the licence accordingly and allow the licence to continue to have effect, as amended until its expiry.

Renewal of Licence

10. (1) A licence under these regulations may be renewed upon an application made to the Authority for renewal of the licence in accordance with the procedure specified in each licence.

(2) The procedure for renewal of a licence shall be the same as that applicable to the grant of the original licence

(3) A licensee who fails to renew its licence or whose application for the renewal is rejected by the Authority shall cease to provide postal or courier services after the expiration of the licence.

Power to amend and suspension of Licence

11.
(1) The Authority may, during the currency of a licence, amend, vary, add to, revoke suspend or revive any condition attached to the

licence or attach new conditions to it and shall notify the licensee in writing within fourteen days.

(2) Where the Authority is satisfied that a licensee is not complying with or has not complied with the conditions of licence, the Authority may suspend or cancel the licence.

(3) The Authority shall notify the licensee in writing of any intended cancellation or suspension of licence, the reasons thereof and timelines for rectification and the action that the Authority intends to take in the event of non-compliance with the notice within the specified timelines.

(4) The Authority shall not suspend or cancel a licence without first giving the licensee an opportunity to be heard and to comply with the directives of the Authority if any, within a reasonable period.

(5) The Authority shall in determining whether it is necessary to suspend or cancel a licence, consider the extent of loss or damage to persons likely to be affected by the suspension or cancellation.

(6) A licence which remains unutilized for six months from the date of its grant shall automatically lapse at the expiry of six months.

Transfer of Licence

12. (1) A licence shall not be transferred except with the prior written approval of the Authority.

(2) An application for approval under sub regulation (1) shall be made by the licensed certification service provider in writing and shall be submitted to the Authority.

(3) An application under sub regulation (1) shall be accompanied by the prescribed fee.

(4) If the licensed certification service provider –
(a) In the case of a company, is wound up
(b) In the case of a partnership being dissolved
(c) In case of an intended merger or acquisition.

(5) The Authority may, on an application in writing, by endorsement on the licence and subject to such conditions as the Authority deems fit, assign the licence to a fit and proper person for the benefit of the licensed certification authority until the expiration of the licence or such earlier date as the Authority thinks

fit and such person shall be deemed to be the licensed certification authority for the purposes of the Act and these Regulations.

PART III-APPROVED DIGITAL SIGNATURE SCHEME AND KEY MANAGEMENT

Approval of Digital Signatures

13. (1) A digital signature scheme shall be approved for the purposes of the Act and these Regulations if-
(a) the digital signature scheme uses a secure public-key algorithm for the generation of the key pair and a secure public-key algorithm and hash function for the creation of the digital signature;
(b) the digital signature scheme satisfies the technical component requirements; and
(c) the digital signature created is not capable of being modified to contain a subliminal channel.

(2) A key pair used to create and verify a digital signature shall not be used to encrypt and decrypt any messages

Storage of Private Keys

14. 1) The data storage medium for the private key may be hardware-based or software-based.

(2) if the data storage medium of the private key is hardware-based, the holder of the private key shall ensure that the token, smart card or other external devices in which the private key is stored is kept in a secure place and a secure manner.

(3) if the data storage medium of the private key is software-based, the holder of the private key shall ensure that the computer system in which the private key is stored is reasonably secure.

(4) The personal identification numbers or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key shall be kept secret.

Disposal of Key Pairs

15. (1) If a key pair is no longer in use or to be used, or if the private key of the key pair is compromised, the holder of the key pair shall dispose of it in a suitable manner, including by destroying it.

(2) A secure means and method shall be used for the destruction of keys.

(3) Notwithstanding sub regulation (1), if the holder desires to retain a key pair that is no longer in use or to be used, or that has

been compromised, the holder shall ensure that the key pair is stored by a reasonably secure method.

PART IV- FOREIGN ELECTRONIC CERTIFICATION SERVICE PROVIDERS

Recognition of foreign Electronic Certification Service Providers

16. The Authority may recognize a foreign electronic certification service provider as an electronic certification service provider for the purposes of these Regulations.

Criterion for Recognition

17. The Authority may recognize a foreign certification service provider as a certification service provider for the purposes of these Regulations, where the foreign certification service provider—:
    (a) Is duly licensed or authorized to issue electronic certification services in the country in which it operates;
    (b) Complies with internationally acceptable standards and requirements under the Act and these Regulations; and
    (c) Has established a local agent to provide certification services in Kenya

Application for Recognition

18. An application for the recognition of a foreign certification service provider as certification service provider for the purposes of these Regulations shall be made to the Authority in writing.

    (2) An application under sub regulation (1) shall be accompanied by –
    (a) proof that the requirements under regulation 17 have been satisfied, including a report from a qualified auditor certifying that the prescribed standards and technical requirements have been satisfied;
    (b) the prescribed fee; and
    (c) such other information or document as the Authority may require

Grant of Recognition

19. (1) On receipt of an application under regulation 17, the Authority shall consider the application.
    (2) If the Authority is satisfied with the qualification and suitability of the foreign certification service provider, the Authority may recognize the foreign certification service provider with or without conditions or may refuse the recognition.
    (3) If the Authority refuses to recognize a foreign certification service provider, the Authority shall immediately notify the applicant in writing of its refusal and the decision of the Authority shall be final.

(4) A certificate issued by an electronic certification service provider recognized under paragraph (1) shall be valid for the purposes of the Act and these Regulations.

Revocation of Recognition

20. (1) The Authority may revoke the certificate of recognition granted under regulation 19 (2) –

(a) if the Authority finds that the recognized foreign certification service provider no longer satisfies the requirements specified under Regulation 17; or

(b) if the recognized foreign certification service provider applies for a revocation of the recognition.

(2) A revocation under sub-regulation (1) shall be by order published in the Gazette.

(3) A revocation under paragraph (1) (b) shall be without prejudice to a fresh application for recognition being made by the foreign certification service provider. Where the Authority is satisfied that a foreign electronic certification service provider has contravened any of the conditions and restrictions of recognition under paragraph (1), it may revoke the recognition.

Application for Revocation of Recognition

21. (1) a recognized foreign certification service provider may apply to the Authority in writing for the revocation of its recognition.

(2) a recognized foreign certification service provider intending to apply for the revocation of its recognition shall, not less than ninety days before the date the application is made, notify all its clients in writing of its intention.

(3) A recognized foreign certification service provider that contravenes sub regulation (2) commits an offence and shall on conviction be liable for a penalty provided in the Act.

Register of Recognized Foreign Electronic Certification Service Providers

22. (1) The Authority shall keep and maintain a Register of recognized foreign electronic certification service providers in such form it may consider fit.

(2) The Authority shall publish a list of recognized foreign certification service providers in such form and manner as it may determine.

PART V- CERTIFICATION PRACTICE STATEMENT

Certification Practice Statement.

23. (1) An electronic certification service provider shall, before the commencement of its operations, prepare a certification practice statement, in accordance with these Regulations and guidelines issued by the Authority from time to time and submit it for approval by the Authority.

(2) An electronic certification service provider shall not change the certification practice statement without the prior written approval of the Authority.

(3) An electronic certification service provider shall specify, in its certification practice statement—
(a) any limitation of its liabilities and particularly, the implication of reliance limitations specified; and
(b) the subscriber identity verification method for the issuance, suspension, revocation and renewal of a certificate.

(4) An electronic certification service provider shall file, with the Authority, a copy of its certification practice statement and specify its effective date and publish it on its website.

(5) An electronic certification service provider shall log all changes to the certification practice statement and specify the effective date of each change.

(6) An electronic certification service provider shall keep, in a secure manner, a copy record of each version of its certification practice statement and record the date it came into effect and the date it ceased to have effect.

Responsibilities of an Electronic Certification Service Provider.

24. (1) An electronic certification service provider shall —
(a) issue and renew certificates;
(b) suspend, reinstate or revoke certificates;
(c) conduct personal identification of subscribers;
(d) publish accurate information relating to certificates;
(e) provide a repository service listing all published certificates, and records of revoked certificates that may be used to verify the validity of published certificates;
(f) ensure the protection of private information and safekeeping of data security; and
(g) provide time-stamp services.

Records management

25. (1) An electronic certification service provider shall keep securely all records relating to —
(a) issuance, renewal, suspension or revocation of certificates, including the identity of any person requesting a certificate;
(b) the process of generating key pairs by the subscribers or the licensed electronic certification service provider;
(c) the administration of its computing facilities; and
(d) such other information as may be determined by the Authority.

(2) A certification service provider may keep its records in paper-based form, electronic form or any other form and avail the records to the Authority in a prescribed manner when it is required.

(3) An electronic certification service provider shall index, store, and preserve the records kept under paragraph (2) in a form that the records may be reproduced in an accurate, complete, legible manner and a manner accessible to the Authority or to any authorized officer.

(4) An electronic certification service provider shall retain a record of all the certificates it has issued and preserve them so that they shall be accessible for a period of not less than seven years.

(5) An electronic certification service provider shall retain all records required to be kept under paragraph (1) and all the logs of the creation of the archive of certificates required under paragraph (3) for a period of not less than seven years.

Issuance of certificates

26. (1) An electronic certification service provider shall issue a certificate containing —

(a) information identifying the electronic certification service provider;

(b) information identifying the signature owner;

(c) signature-verification data which corresponds to signature-creation data;

(d) the commencement and expiry date of the certificate;

(e) information regarding the authorization of the subscriber, if a subscriber is acting on behalf of another person;

(f) information regarding the conditions of usage of the certificate and limits on the value of transactions, where applicable;

(g) the secure electronic signature of the electronic certification service provider that verifies the information in the certificate;

(h) sufficient information that can be used to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate would be listed if the certificate is suspended or revoked; and

(i) any other information as may be determined by the Authority from time to time.

(2) An electronic certification service provider shall determine, based on official documents, the identity of the person to whom a certificate is issued and shall specify, in the certification practice statement, the subscriber identity verification method applied in the issuance of certificates.

(3) An electronic certification service provider shall—
(a) give a subscriber an opportunity to verify the contents of the certificate before the subscriber accepts it;
(b) inform a subscriber, in writing, of the legal effect of an advanced electronic signature, the limitations on the use of certificates and the dispute resolution procedures, applicable;
(c) warn subscribers, in writing, not to allow third parties to use signature creation data associated with signature verification data in the certificate.

(4) Where the subscriber accepts the issued certificate, the electronic certification service provider shall publish a signed copy of the certificate in a repository in accordance with regulation 27 (2).

(5) Where the subscriber does not accept the certificate, the electronic certification service provider shall not publish the certificate.

(6) Once a certificate has been issued by the electronic certification service provider and accepted by the subscriber, the electronic certification service provider shall notify the subscriber, within a reasonable time, of any fact that subsequently becomes known to the electronic certification service provider that may significantly affect the validity or reliability of the certificate.

(7) An electronic certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the issuance of a certificate.

(8) Where an electronic certification service provider issues an additional certificate to a person based on a valid certificate held by the same person and subsequently the original certificate is suspended or revoked, the certification service provider shall investigate and determine whether the new certificate should also be suspended or revoked.

Obligations of a subscriber

27. (1) Where a subscriber has accepted a certificate, the subscriber shall generate a key pair by applying the relevant security procedure.

(2) A subscriber shall be deemed to have accepted a certificate if he publishes or authorizes the publication of the certificate to any person, in a repository; or otherwise demonstrates his acceptance.

(3) A subscriber certifies, by accepting a certificate, to all who wish to reasonably rely on the information contained in the certificate that—
(a) the subscriber holds and is entitled to hold the private key corresponding to the public key listed in the certificate;
(b) all representations made by the subscriber to the electronic certification service provider and all the information contained in the certificate are true; and
(c) all information in the certificate is within the knowledge of the subscriber and is true.

(4) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his certificate and take the necessary steps to prevent its disclosure to any person who is not authorized to affix the advanced electronic signature of the subscriber.
(5) In the event that the subscriber becomes aware that the private key has been compromised, the subscriber shall notify the certification service provider of such compromise within twenty-four hours.

Liability of Electronic Certification Service Providers

28. (1) An electronic certification service provider shall, by issuing or guaranteeing a certificate to the public, accept liability for damage caused to any person who reasonably relies on the certificate unless the electronic certification service provider can prove that it was not negligent.

(2) The liability of an electronic certification provider under paragraph (1) shall be limited to issues relating to—
(a) the accuracy, at the time of issuance, of all information contained in the certificate and the fact that the certificate contains all the details prescribed for the certificate;
(b) the assurance that at the time of issuance of the certificate, the signatory identified in the certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
(c) assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the electronic certification service provider generated both of them; and
(d) the failure to publish a notice of suspension or revocation of a certificate in the repository specified in the certificate.

(3) Where an electronic certification service provider has specified in a certificate, the limits on the use of the certificates and the limits on the values of transactions for which the certificate may be used,

it shall put in place mechanisms to revoke the validity of the subscriber's certificate and will not be liable for any damage resulting from exceeding the limits.

Renewal of certificates

29. (1) The subscriber identity verification method employed for the renewal of certificates shall be specified in the certification practice statement.

(2) A certification service provider shall log and keep, in a secure manner, the date and time of all transactions relating to the renewal of a certificate.

Suspension of certificates

30. (1) An electronic certification service provider shall maintain facilities that can receive and respond to requests for suspension of certificates at all times of the day and on all days of every year.

(2) An electronic certification service provider shall, upon receiving a valid request under paragraph (1) suspend a certificate and publish a notice of the suspension in the respective repository.

(3) The subscriber identity verification method employed for the suspension of certificates shall be specified in the certification practice statement.

(4) Where a request for suspension is received and an electronic certification service provider determines the revocation of the certificate would be justified in the light of all the evidence available to it, the electronic certificate service provider may revoke the certificate.

(5) An electronic certification service provider may, regardless of the subscriber's consent, suspend a certificate that it has issued if it has reasonable grounds to believe that the certificate is unreliable:
Provided that the electronic certification service provider shall conduct and complete its investigation into the reliability of the certificate and decide within a reasonable time whether to reinstate or revoke the certificate.

(6) An electronic certification service provider shall, within a reasonable time, terminate a suspension initiated through a request, upon discovering and confirming that the request for suspension was made without the authorization of the subscriber.

(7) An electronic certification service provider shall, after suspending a certificate, consult and engage with the subscriber or

his authorized agent to determine whether to reinstate or revoke the certificate.

(8) An electronic certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the suspension of certificates.

(9) A party who wishes to rely on any certificate shall, before relying on a certificate, establish the status of the certificate.

Revocation of certificates

31. (1) An electronic certification service provider shall revoke a certificate upon —

(a) receiving a request for revocation from a subscriber or his authorized agent;

(b) detecting forgery or falsification of the information existing in the database or changes in the information in the database; and

(c) detecting the incapacity, bankruptcy or death of the subscriber:

Provided that where it is practicable, an electronic certification service provider shall afford the subscriber a reasonable opportunity to be heard, before the revocation is effected.

(2) An electronic certification service provider shall maintain facilities that can receive and act upon requests for revocation at all times of the day and on all days of every year.

(3) An electronic certification service provider shall use the subscriber identity verification method specified in the certification practice statement to confirm the identity of the subscriber or authorized agent who makes a request for revocation.

(4) An electronic certification service provider shall, after revoking a certificate, give notice of revocation to the subscriber and publish the notice in the respective repository.

(5) An electronic certification service provider shall log and keep in a secure manner the date and time of all transactions relating to the revocation of a certificate.

(6) A party who wishes to rely on any certificate shall, before relying on a certificate, establish the status of the certificate from the service provider.

Performance audits

32. The Authority shall, at least once every year, audit the operations of a licensed electronic certification service provider to monitor compliance with the Act and these Regulations.

Security Guidelines

33. (1) An electronic certification service provider shall comply with the security Guidelines that may be issued by the Authority.

(2) An electronic certification service provider shall provide every subscriber with a secure and trustworthy system to generate his key pair.

(3) An electronic certification service provider shall establish a mechanism that generates and verifies advanced electronic signatures in a secure and trustworthy manner and indicates the validity of a signature.

(4) Where the advanced electronic signature is not valid, the mechanism established under paragraph (3) should indicate the reason for invalidity and the status of the certificate.

(5) Where a verification mechanism is established by any person who is not an electronic certification service provider, the resulting signature shall not be considered secure unless a licensed electronic certification service provider endorses the implementation of the mechanism and its certificate.

(6) A licensed electronic certification service provider shall store the keys, including the subscriber's and the electronic certification service provider's keys, in a secure and trustworthy manner.

Incident handling

34. An electronic certification service provider shall establish an incident management plan to address, among others, incidents relating to—

(a) compromise of key;

(b) penetration of electronic certification service provider's system and network;

(c) unavailability of infrastructure; and

(d) fraudulent registration and generation of certificates, certificate suspension and revocation information.

(2) Where any incident referred to in paragraph (1) occurs, an electronic certification service provider shall report the incident to the Authority within twenty-four hours.

(3) The Electronic certification service providers shall comply with the provisions of the Kenya Information and Communications (Consumer Protection) Regulations 2023 in relation to Consumer Complaints Resolution. The Subscribers shall escalate any

complaints to the Authority if dissatisfied with the resolution offered by the service provider.

Confidentiality

35. 1) An electronic certification service provider shall not collect personal data directly from the subscribers or their authorized agents unless the personal data is necessary for the purposes of issuance of a certificate and the collection is consistent with the provisions of the Data Protection Act, 2019.

(2) An electronic certification service provider shall keep all information relating to a subscriber confidential.

(3) An electronic certification service provider shall not disclose or share any information relating to a subscriber unless the disclosure is authorized by the subscriber:
Provided that an electronic certification service provider may, pursuant to an order of the court, disclose information relating to a subscriber without the consent of the subscriber. The subscriber should however be notified by the service provider of the court order's demand.

(4) The obligation to maintain confidentiality shall not apply to information relating to a subscriber which —
(a) is contained in the certificate and is available to the public for inspection;
(b) is otherwise provided by the subscriber to the licensed electronic certification service provider for disclosure to the public; or
(c) relates to the revocation or suspension of a certificate.

(5) Where an electronic certification service provider has permitted a subscriber to use a pseudonym, the electronic certification service provider shall, at the request of law enforcement authorities, disclose data relating to the subscriber that is required to prosecute offences or to protect against threats to public safety or public order.

Winding up of operations of an Electronic Certification Service Provider

36. (1) An electronic certification service provider may, where the electronic certification service provider intends to discontinue its operations—
(a) arrange for its subscribers to re-subscribe to be on-boarded by another licensed electronic certification service provider;
(b) make arrangements for its records and certificates to be archived in a secure manner; and
(c) transfer its records to another licensed electronic certification service provider in a secure manner.

((2) An electronic certification service provider shall, where the electronic certification service provider intends to discontinue its operations—

(a)give the Authority and its subscriber a minimum of six months' notice, in writing, of its intention to discontinue its operations; and

(b)publish, in at least one local daily newspaper with nationwide circulation and in such other manner as the Authority may determine, at least two six months' notice of its intention to discontinue its operations.

PART VI -MISCELLANEOUS PROVISIONS

Offences

37. A person who contravenes these Regulations commits an offence and shall be liable to a penalty as provided for under the Act.

PART VII – REPEAL, SAVINGS AND TRANSITIONAL PROVISIONS

Revocation

38. The Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 are hereby revoked.

Preservation of proceedings and rights of appeal

39. Any proceedings, instruments and any right of review or appeal subsisting immediately before the commencement of these Regulations by virtue of the repealed regulations shall after the commencement of these Regulations be treated as subsisting by virtue of the corresponding enactment in these Regulations.

Continuance of periods of time

40. Where a period of time specified in the repealed Regulations is current at the commencement of these Regulations, these Regulations shall have effect as if the corresponding provisions had been in force when the period began to run.

Dated the …….2023

Eliud Owalo
Cabinet Secretary for Information, Communications and the Digital Economy