Draft – 9 February 2024

**Electronic Transactions and Cyber Security (CERTIFICATION AUTHORITY AND ENCRYPTION) Regulations, 2024**

# **Electronic Transactions and Cyber Security (CERTIFICATION AUTHORITY AND ENCRYPTION) Regulations, 2024**

# ARRANGEMENT OF REGULATIONS

# PART I—PRELIMINARY

1. Citation
2. Interpretation
3. Application and interpretation of inconsistent terminology

# PART II— ACCREDITATION OF CERTIFICATION AUTHORITIES

1. Types of accreditations
2. Effect of an accreditation
3. Validity periods
4. Application procedures
5. Application fees
6. Granting of an accreditation
7. Renewal of an accreditation
8. Eligibility requirements

# PART III— CERTFICATION AUTHORITY OPERATIONS

1. Issuance and renewal of certificates
2. Suspension of certificates
3. Revocation of certificates
4. Certification practice statements
5. Trustworthy transaction logs, recordkeeping and archives
6. Reporting
7. Incident handling
8. Trusted persons
9. Data security
10. Confidentiality and data protection
11. Discontinuation of operations

# PART IV—ENFORCEMENT

1. Enforcement

# PART V— ENCRYPTION SERVICES AND PRODUCTS

1. Limitations on restrictions
2. Registration of certain providers
3. Restrictions on import, export or use of encryption products
4. Declarations of technical characteristics and source code

# PART VI—INTERPRETIVE CLARIFICATIONS

1. Interpretive clarifications

# PART VII—MISCELLANEOUS

1. Appeals of orders, decisions or determinations of the Authority
2. Invalidity not to affect enforceability

GOVERNMENT NOTICE NO. …

…………………….

# **Electronic Transactions and Cyber Security (CERTIFICATION AUTHORITY AND ENCRYPTION) Regulations, 2024**

IN EXERCISE of the powers conferred by sections 12(2), 51, 52, 67 and 102 of the Electronic Transactions and Cyber Security Act, 2016, I, Moses Kunkuyu, Minister of Information and Digitalization, on advice of the Malawi Communications Regulatory Authority, make the following Regulations—

# PART I—PRELIMINARY

Citation

1. These Regulations may be cited as the Electronic Transactions and Cyber Security (Certification Authority and Encryption) Regulations, 2024.
2. In these Regulations, unless the context otherwise requires—

Interpretation

“accreditation” means a licence or authorisation issued by the Authority to a certification authority under these Regulations, as further described in regulation 4;

“accredited certification authority” means a certification authority that holds a valid accreditation from the Authority;

“certification practice statement” means a statement prepared by a certification authority that governs its methodology in the issuance, suspension, revocation and renewal of certificates and other matters addressed in regulation 15;

“consent” means specific, informed and unambiguous agreement or approval by a person, or another person who has the authority to provide the consent on behalf of the first person, given freely, in writing, orally or by any affirmative action;

“license” has the meaning described in regulation 4;

“recognition” has the meaning described in regulation 4;

“restricted encryption services or products” means those encryption services or products or classes of encryption services or products, the providers of which are required to register to the Authority under regulation 25;

“subscriber” means a person who is the subject named or identified in a certificate issued to that person and who holds a private key that corresponds to a public key listed in that certificate;

“trusted person” means any natural person employed by a certification authority who has—

direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Regulations; or

duties directly involving the issuance, renewal, suspension or revocation of certificates (including the identification of any person requesting a certificate from a certification authority), creation of private keys or administration of a certification authority’s computing facilities.

1. (1) These Regulations shall apply to—

Application and interpretation of inconsistent terminology

1. accredited certification authorities;
2. any other certification authorities operating in Malawi, except where otherwise indicated that a particular provision or obligation applies only to accredited certification authorities; and
3. persons providing, importing, exporting or using encryption services or products in Malawi.
4. As more fully described in Part VI these Regulations interpret and reconcile inconsistent terminology used in the Act.

# PART II—ACCREDITATION OF CERTIFICATION AUTHORITIES

Types of accreditations

1. (1) The Authority may issue one of two types of accreditations to a certification authority—
2. a license; or
3. an authorisation in the form of a recognition.

1. To be eligible for a license, an applicant shall demonstrate that it is registered as a company under the Companies Act or such other act providing for the registration of organisations under the laws of Malawi.

Cap. 46:03

1. To be eligible for a recognition, an applicant shall demonstrate that it is a foreign certification authority that—
2. it is duly registered as a company or other organisation in its home jurisdiction;
3. it has established a local agent in Malawi acceptable to the Authority; and
4. either—
5. it is validly accredited as a certification authority by the relevant competent entity in its home jurisdiction; or
6. no such accreditation is required to operate as a certification authority in its home jurisdiction
7. (1) If a digital certificate is issued by person that is not an accredited certification authority, such digital signature shall not satisfy sections 46(b)(i) or 46(b)(ii) of the Act for purposes of establishing it as a secure electronic signature under the Act.

Effect of an accreditation

1. Notwithstanding subregulation (1), and consistent with section 12(1) of the Act, nothing in these Regulations shall be interpreted to prevent—
2. a certification authority from operating in Malawi without an accreditation; or
3. a person from using the services of a certification authority on the basis that it lacks an accreditation.
4. (1) The Authority shall from time to time establish the validity periods for each type of accreditation set out in regulation 44, including renewals.

Validity periods

1. Notwithstanding subregulation (1), the validity period of an accreditation shall not be less than one year.
2. Any reduction to the validity period established by the Authority pursuant to subregulation (1) shall be prospective only and shall not affect the validity period of any existing accreditation.
3. In its discretion, the Authority may make any increase to the validity period established by the Authority pursuant to subregulation (1) applicable to one or more existing accreditations.
4. Notwithstanding subregulation (3), a reduction or increase in the validity period established by the Authority for renewals shall apply to renewals of existing accreditations.

1. (1) Any eligible person that wishes to apply for an initial accreditation or to renew an existing accreditation shall do so through submission of a written application in the manner prescribed by the Authority.

Application procedures

1. An applicant for an initial accreditation or a renewal of an accreditation shall submit a copy of its certification practice statement which meets the requirements of regulation 15 and the Act as part of its application.
2. The Authority shall, from time to time, issue accreditation guidelines prescribing—
3. eligibility requirements of applicants in addition to those set out in these Regulations;
4. application forms for each accreditation type, including renewals;
5. information, documentation and written statements of fact required to accompany an application for each accreditation type, including renewals;
6. additional accreditation procedures to supplement those set out in these Regulations; and
7. any other matter relating to accreditation of certification authorities that is not inconsistent with the Act or these Regulations.
8. An applicant for an accreditation shall be bound by all terms, commitments, offers, presentations, proposals, plans and obligations stated in its application and shall ensure the accuracy of all documents, information and written statements of fact submitted and representations made as part of the application.

1. (1) An application submitted pursuant to regulation 7 shall be accompanied by payment of a non-refundable application fee in an amount, and submitted in a manner, prescribed by the Authority.

Application fees

1. The prescribed application fees may vary depending on whether the application relates to an initial accreditation or a renewal, the type of accreditation and the validity term of the accreditation sought.

1. (1) The Authority shall consider each complete application submitted and notify the applicant of its determination within [ninety] days from the date of receipt of a completed application.

Granting of an accreditation

1. An application shall not be deemed complete until after the Authority has received payment of the required application fee under regulation 8.
2. Where an applicant submits an application that fails to provide documents, information or written statements of fact as required by the Authority—
3. the application shall not be considered complete;
4. the Authority shall inform the applicant of the above facts in writing, within fourteen days; and
5. the applicant may submit to the Authority the missing documents, information or written statements of fact as required by the Authority to make the application complete.
6. In evaluating an application for an accreditation, the Authority shall consider—
7. the eligibility requirements for each type of accreditation set out in regulation 11; and
8. whether granting the accreditation would be in the public interest.
9. Upon any grant or renewal of accreditation, the Authority shall—
10. publish notice of the grant or renewal in the *Gazette*; and
11. note the grant or renewal in the register of accredited certification authorities kept and maintained by the Authority pursuant to section 51(3) of the Act.
12. The Authority shall maintain and publish an up-to-date list of all currently accredited certification authorities on its website, accessible to the public.
13. (1) Unless otherwise provided in the terms and conditions of the accreditation or instructed by the Authority in writing, a certification authority shall apply for a renewal of an accreditation no later than [ninety] days prior to the expiry of its validity period.

Renewal of an accreditation

1. When considering an application for renewal of an accreditation, the Authority shall have regard to whether—
2. the certification authority has operated in accordance with its existing and prior accreditations;
3. the certification authority continues to meet eligibility requirements under the Act and these Regulations;
4. the certification authority continues to be financially and operationally capable of meeting its obligations under the Act and these Regulations;
5. the certification authority has not, during the validity period of its current or any prior accreditation, contravened the provisions of the Act, these Regulations, the conditions of such accreditation or any applicable requirements issued by the Authority or any other relevant laws; and
6. the renewal of the accreditation would be in the public interest.
7. In its discretion, the Authority may renew an accreditation with no or minimal changes to the accreditation or impose new terms and conditions that it deems are in the public interest.

1. (1) To be eligible for an accreditation, an applicant shall demonstrate as part of its application that it meets, and will be able to meet for the expected validity period of the accreditation, the following requirements—

Eligibility requirements

1. the eligibility requirements of regulation 4(3) and 4(4), as applicable;
2. the obligations of certification authorities and accredited certification authorities set out in Part III and otherwise in the Act;
3. that it is in a sound financial position in proportion to the size of its business;
4. that it has adequate insurance against liability for such sum as may be determined by the Authority for each claim arising out of any error or omission on the part of the applicant, its officers or employees; and
5. any further eligibility requirements established by the Authority under regulation 7(3), including but not limited to any requirement to undergo an audit by a qualified third party to confirm some or all of the eligibility requirements.

# PART III— CERTFICATION AUTHORITY OPERATIONS

1. (1) In addition to the requirements of section 55 of the Act, a certification authority shall comply with the requirements of this regulation 12 in relation to the issuance of certificates and the renewal of certificates.

Issuance and renewal of certificates

1. A certification authority shall provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted by the subscriber.
2. If a subscriber accepts an issued or renewed certificate, the certification authority shall publish a signed copy of the certificate unless the certification authority and subscriber contractually agree otherwise.
3. If a subscriber does not accept a certificate, the certification authority shall not publish it
4. It is the responsibility of any person relying on a certificate to check the appropriate repository or registers under sections 60 and 61 of the Act to determine whether an issued certificate has been suspended or revoked.
5. Once a certificate has been issued or renewed by a certification authority and accepted by a subscriber, the certification authority shall notify the subscriber within a reasonable time of any fact known to the certification authority that significantly affects the validity or reliability of the certificate
6. Where a certificate is issued or renewed to a person on the basis of another valid certificate held by the same person and subsequently the originating certificate has been suspended or revoked, the certification authority that issued the new certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new certificate.
7. A certification authority shall log and keep the date and time of all transactions in relation to the issuance or renewal of a certificate in a trustworthy manner.
8. A certification authority shall ensure that every certificate states the date on which it expires.
9. (1) Where a subscriber, or a person acting on behalf of the subscriber where the subscriber is not available, makes a request for suspension of a certificate under section 57 of the Act, the certification authority shall use the subscriber identity verification method specified in its certification practice statement to confirm the identity of the subscriber or person acting on the subscriber’s behalf making the request.

Suspension of certificates

1. A certification authority shall, after verifying the identity of the subscriber, or person acting on the subscriber’s behalf, and being satisfied that a request for suspension is validly made, suspend the certificate and publish a signed notice of the suspension in accordance with section 60 of the Act.
2. A certification authority shall inform the subscriber, or the person acting on the subscriber’s behalf, whether a suspended certificate shall be revoked under subregulation (7) or reinstated after suspension.
3. A certification authority shall terminate a suspension initiated by request if the certification authority discovers and confirms that the request for suspension was made without authorisation by the subscriber, or the person acting on the subscriber’s behalf.
4. A certification authority may additionally suspend a certificate that it has issued and publish a signed notice of the suspension in accordance with section 60 of the Act if the certification authority upon an investigation has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber requests or consents to the suspension.
5. A certification authority shall complete its investigation under subregulation (5) and decide within a reasonable time whether to reinstate the certificate or to revoke the certificate under subregulation (7).
6. If a certification authority considers that revocation of a suspended certificate pursuant to section 58 or 59 of the Act is justified in the light of all the evidence available to it, the certificate authority shall revoke the certificate in accordance with the requirements of the Act and regulation 14.
7. A certification authority shall log and keep the date and time of all transactions in relation to the suspension of certificates in a trustworthy manner.
8. A certification authority shall maintain facilities to receive and act upon requests for suspension under section 57 of the Act at all times of the day and on all days of the year.

1. (1) Where a subscriber or the subscriber’s representative makes a request for revocation of a certificate under section 58(a) of the Act, the certification authority shall use the subscriber identity verification method specified in its certification practice statement to confirm the identity of the subscriber or the subscriber’s representative making the request.

Revocation of certificates

1. A certification authority shall, after verifying the identity of the subscriber or the subscriber’s representative pursuant to subregulation (1) and being satisfied that a request for revocation is validly made, revoke the certificate and publish a signed notice of the suspension in accordance with section 61 of the Act.
2. A certification authority may additionally revoke a certificate on any of the other grounds set out in sections 58 (b), (c) and (d) and section 59 of the Act and publish a signed notice of the suspension in accordance with section 61 of the Act.
3. Upon any revocation of a certificate, a certification authority shall give notice to the subscriber immediately upon the revocation of a certificate, except where such notification is not practical in the case of revocation as a result of the subscriber’s death, dissolution or other cessation of existence under section 58(b), (c) and (d) of the Act.
4. A certification authority shall log and keep the date and time of all transactions in relation to the revocation of certificates a trustworthy manner.
5. A certification authority shall maintain facilities to receive and act upon requests for revocation under section 58(a) of the Act at all times of the day and on all days of the year.

1. (1) A certification authority shall have, maintain and comply with a certification practice statement that—

Certification practice statements

1. specifies a subscriber identity verification method that it uses for the issuance, suspension, revocation and renewal of certificates and that is acceptable to the Authority;
2. includes practices and procedures that meet all of the conditions specified in section 55(2) of the Act; and
3. conforms to any other applicable requirements established by the Authority.
4. An accredited certification authority shall submit a copy of its certification practice statement to the Authority within [thirty] days of making any changes or updates thereto.
5. An accredited certification authority shall publish the current version of its certification practice statement together with its effective date on the certification authority’s website.

1. (1) A certification authority shall make and keep in a trustworthy manner records relating to—

Trustworthy transaction logs, recordkeeping and archives

1. activities relating to the issuance, renewal, suspension and revocation of certificates, including the process of identification of any person requesting a certificate from the certification authority;
2. the process of generating subscribers’ or the certification authority’s own key pairs;
3. the administration of the certification authority’s information systems; and
4. such other activities of the certification authority as may be determined by the Authority.
5. A certification authority shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of not less than 10 years from the date of expiration of the certificate.
6. A certification authority shall retain all records required to be kept under subregulation (1) and all logs of the creation of the archive of certificates referred to in subregulation (2) for a period of not less than 10 years.
7. A certification authority may keep its records and logs under this regulation 16 in the form of paper documents, electronic records or any other form approved by the Authority.
8. The records and logs of a certification authority under this regulation 16 shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to the Authority or a third-party auditor.
9. (1) An accredited certification authority shall submit an annual report and annual financial statements to the Authority.

Reporting

1. The annual reports shall include information on—
2. the number of subscribers;
3. the number of certificates issued, suspended, revoked, expired and renewed;
4. system performance including system up and down time and any extraordinary incidents;
5. changes in the organisational structure of the accredited certification authority;
6. changes since the preceding report was submitted or since the most recent application for an accreditation; and
7. changes in the particulars of any trusted person since the last submission to the Authority, including the name, identification number, residential address, designation, function and date of employment of the trusted person.
8. The Authority may further specify specific items to be included in or the format of the annual report or the annual financial statements.
9. (1) A certification authority shall implement an incident management plan that shall provide at the least for management of the following incidents—

Incident handling

1. compromise of key;
2. unauthorised or unlawful penetration of the certification authority’s system and network;
3. unavailability of infrastructure; and
4. fraudulent registration, generation, use, suspension or revocation of certificates.
5. An accredited certification authority shall report any incident referred to in subregulation (1) to the Authority within 24 hours of becoming aware of such incident.
6. A certification authority shall take reasonable measures to ensure that every trusted person—

Trusted persons

1. is a fit and proper person to carry out the duties assigned;
2. is not an undischarged bankrupt in Malawi or elsewhere; and
3. has not been convicted, whether in Malawi or elsewhere, of—
4. an offence involving fraud or dishonesty; or
5. an offence under the Act, the under the Communications Act or the Data Protection Act;

Cap. 68:01 Cap. [ ]

1. has good knowledge of the Act and these Regulations;
2. is trained in the certification authority’s certification practice statement; and
3. possesses the relevant technical qualifications, expertise and experience to effectively carry out the duties assigned.
4. (1) A certification authority shall establish policies and procedures, including adequate technical and administrative measures, to ensure the integrity, confidentiality and availability of information employed in its operations and the availability of its services, including without limitation with respect to the classification, labelling, storage, access and destruction of information according to its value, sensitivity and importance in the operations of the certification authority.

Data security

1. The Authority may issue guidelines establishing specific measures or standards that a certification authority shall meet in satisfying subregulation (1).
2. (1) A certification authority shall keep all subscriber-specific information confidential and not disclose any subscriber-specific information without prior consent of the subscriber, except—

Confidentiality and data protection

1. where the subscriber-specific information—
2. is included in a certificate for public disclosure;
3. is otherwise provided to the certification authority for public disclosure; or
4. relates to the fact that a certificate has been suspended or revoked;
5. in compliance with an order of a court or the requirement of any written law; or
6. in compliance with a request for information by the Authority in furtherance of its powers to conduct an investigation under Part IV where any such subscriber-specific information is necessary for the Authority to conduct its investigation.
7. Without limiting the obligations or the scope of the exceptions under subregulation (1), a certification authority shall otherwise comply with the obligations of a “data controller,” and, where applicable, the obligations of a “data controller of significant importance,” with respect to processing of “personal data” of a subscriber (or, in the case of a subscriber that is an entity, any natural person associated with such subscriber) under the Data Protection Act.

Cap. [ ]

1. Where a certification authority intends to discontinue its operations, it shall—

Discontinuation of operations

1. arrange for its subscribers to have the opportunity to re-subscribe to another certification authority;
2. ensure that its records and certificates are archived in a trustworthy manner;
3. provide its subscribers with no less than sixty days’ written notice of its intention to discontinue operations;
4. advertise in such daily newspaper and in such manner as the Authority may determine, its intention to discontinue its operations no less than sixty days prior to the discontinuation; and
5. in the case of an accredited certification authority, provide the Authority with no less than ninety days’ written notice of its intention to discontinue operations.

# PART IV—ENFORCEMENT

Enforcement

1. (1) Where there is a complaint made against a certification authority or the Authority suspects that a certification authority is contravening or has contravened the Act, these Regulations or any condition of an accreditation, the Authority shall commence investigations into such complaint or suspicion for the purpose of securing compliance with the Act, these Regulations or the condition in question.
2. Where the investigations under subregulation (l) indicate that there is a likely breach of a condition of the Act, these Regulations or any condition of an accreditation, the Authority shall make its determination on the matter.
3. The Authority may at any time issue an interim order directing a certification authority to stop specific conduct or to take a specific act where the Authority is satisfied that—
4. there is *prima facie* evidence that the certification authority contravened the Act, these Regulations or any condition an accreditation;
5. continuation of the certification authority’s conduct is likely to cause serious harm to other certification authorities, consumers or the general public;
6. the potential harm in allowing a certification authority to continue its conduct outweighs the burden on the certification authority; or
7. issuing the order is in the public interest.
8. Where the Authority determines that a certification authority has contravened the Act, these Regulations or any condition of an accreditation, the Authority may impose any of the following regulatory sanctions—
9. in the case of an accredited certification authority, revoke the accreditation of the certification authority;
10. in the case of an accredited certification authority, suspend the accreditation of the certification authority for such period, or until the happening of such event, as the Authority may determine;
11. reprimand or issue a warning to the certification authority;
12. issue an order for compliance with the Act, these Regulations or a condition of an accreditation;
13. issue an order to cease operations as a certification authority in Malawi;
14. impose administrative penalties under section 101 of the Act; or
15. make any other order it considers appropriate.
16. When imposing a regulatory sanction, under subregulation (4), the Authority shall consider any aggravating factors involved, including—
17. the gravity of the contravention;
18. the duration of the contravention;
19. whether the contravention resulted in injury to a person or property;
20. whether the certification authority has a previous history of contraventions; or
21. whether the certification authority is a repeat offender.
22. When imposing a regulatory sanction under subregulation (4) the Authority may, consider any mitigating factors involved, including—
23. whether the contravention is minor;
24. whether the consequence from the violation is minor;
25. whether the certification authority took prompt action to correct the contravention;
26. whether the contravention was accidental; or
27. whether the certification authority voluntarily disclosed the contravention to the Authority.
28. The Authority shall in all cases of enforcement impose regulatory sanctions that significantly deter impermissible conduct, but these sanctions shall be proportionate to the severity of the contravention.
29. Upon any suspension or revocation of an accreditation, the Authority shall—
30. publish notice of the revocation or suspension of an accreditation in the *Gazette*;
31. note the revocation or suspension in the register of certification authorities kept and maintained by the Authority pursuant to section 51(3) of the Act; and
32. note the revocation or suspension on the list of validly accredited certification authorities maintained on its website under regulation 9(6).

# PART V—ENCRYPTION SERVICES AND PRODUCTS

Limitations on restrictions

1. Except as required by the subsequent regulations in this Part or otherwise by law, no person shall—
2. be required to register to the Authority under section 52(1) and (2) of the Act;
3. be subject to restrictions or prohibition on the import, export or use of encryption programmes or encryption products under section 52(3) of the Act;
4. be required to declare to the Authority the technical characteristics of any encryption means or the source code used in any encryption services under section 67 of the Act.

1. (1) The Minister may, on the basis of compelling national defence or internal security concerns and after consultation with the Authority, designate by publication in the *Gazette* one or more encryption services or products or classes of encryption services or products that shall be considered restricted encryption services or products, respectively, the providers of which shall be required to register to the Authority under section 52(1) and (2) of the Act.

Registration of certain providers

1. Any designation under subregulation (1) shall set out the prescribed manner and form of the registration and any applicable registration fees.
2. (1) Consistent with section 52(3) of the Act, the Minister may, on the basis of compelling national defence or internal security concerns and after consultation with the Authority, designate by publication in the *Gazette* one or more encryption programmes or encryption products or classes of encryption programmes or encryption products whose import, export or use may be restricted or prohibited.

Restrictions on import, export or use of encryption products

1. Any designation under subregulation (1) shall set out the specific restrictions or prohibitions on the import, export or use of such encryption programmes or encryption products.
2. (1) Consistent with section 67(1) and (2) of the Act, the Minister may, on the basis of compelling national defence or internal security concerns and after consultation with the Authority, designate by publication in the *Gazette* one or more encryption services or class of encryption services, the providers of which shall be required to declare to the Authority the technical characteristics of the encryption used in the services as well as the source code of the software used in the provision of such services.

Declarations of technical characteristics and source code

1. Any designation under subregulation (1) shall set out the prescribed manner and form of such declarations.

# PART VI—INTERPRETIVE CLARIFICATIONS

1. The Authority shall consider the following clarifications when interpreting the provisions of the Act—

Interpretive clarifications

1. the term “certification authority” in the Act shall be interpreted to include any person that issues digital certificates in Malawi used to create digital signatures and public-private key pairs, regardless of whether such person is licensed or authorized by the Authority;
2. an accreditation under these Regulations shall constitute an approval of a certification authority by the Authority for purposes of section 12(2) of the Act;
3. the reference to a “licensed certification authority” in section 47 of the Act shall apply to all accredited certification authorities, including those accredited with an authorization in the form of a recognition under these Regulations.
4. the reference to “the prospective subscriber” having a certification practice statement in section 55(1)(b) of the Act shall be considered a clear error in drafting and interpreted as a reference to “the certification authority;”
5. the reference to “cryptograph services or products” in sections 52(1) and 52(2) of the Act shall be interpreted to apply only to restricted encryption services or products.

# PART VII—MISCELLANEOUS

1. A person who is not satisfied with any order, decision or determination of the Authority made under these Regulations may appeal to the High Court within thirty days from the date the order, decision or determination was made.

Appeals of orders, decisions or determinations of the Authority

1. Where one or more of the provisions of these Regulations becomes invalid or unenforceable, that fact itself shall not affect the validity or enforceability of the other provisions of these Regulations.

Invalidity not to affect enforceability

Made this day of 2024.

Moses Kunkuyu

Minister of Information and Digitalization