National Digital Economy and E-Governance Bill, 2025

Arrangement of Sections

A Bill for an Act to enable the growth of the digital economy and digital governance in Nigeria by facilitating electronic transactions and communications, digital service delivery, and matters related.

CHAPTER ONE – OBJECTIVES, SCOPE, AND APPLICATIONS

PART I – OBJECTIVE AND APPLICATION

1. Objectives

The objectives of this Act are to —

(a) strengthen legal certainty and promote public confidence in the integrity and reliability of electronic transactions, communications and records;

(b) promote and facilitate the utilisation of information and communication technology by public institutions to—

(i) enhance service delivery to citizens,

(ii) strengthen the efficiency and effectiveness of government processes, procedures and systems, and

(iii) foster transparency, openness, and accountability;

(c) reform, harmonise, and amend existing legislation as necessary to facilitate and accelerate the digital economy in Nigeria; and

(d) provide a regulatory framework for the development, implementation, and responsible use of artificial intelligence systems and other emerging technologies.

2. Application

The provisions of this Act shall apply to –

(a) persons and public institutions in respect of their electronic transactions, communications, and records governed by the laws of the Federal Republic of Nigeria;

(b) trust service providers, whether established within or outside Nigeria, in respect of the services they provide, enable, or support within Nigeria;

(c) public institutions as it relates to their processes, procedures, and systems; and

(d) artificial intelligence agents and emerging technologies agents as defined under this Act.

CHAPTER TWO - ELECTRONIC TRANSACTIONS, COMMUNICATIONS AND RECORDS

PART II –ELECTRONIC RECORDS

3. Request to provide access to information in paper form, and information in original form

(1) Where any law requires —

(a) the provision of access to information that is in paper or other non-electronic form, or provides for certain consequences if the information is not made available in the required paper or printed form;

(b) information to be presented or retained in its original form, or provides for certain consequences if the information is not presented or retained in such form;

such a requirement shall be met if any of these activities are rendered, performed, or made in an electronic form and the conditions contained in subsection (2) of this section are satisfied.

Provided that, as it relates to subsection (1) (b) of this section, the provisions of this section shall not apply to any law that regulates evidential matters in judicial proceedings.

(2) Where in pursuance of subsection (1) of this section an activity is performed in an electronic form, the following conditions must be satisfied —

(a) in the case of subsection (1) (a) of this section, the form and means of access to the information must reliably ensure the maintenance of the integrity of the information pursuant to section 37, given the purpose and circumstances in which access to the information is required to be provided.

(b) in the case of subsection (1) (b) of this section, the information contained in the electronic form is accessible and usable for subsequent reference, and the integrity of the information shall, pursuant to section 37, be determined in its final form as an electronic record.

(3) Where subsection (1)(a) of this section applies, a legal requirement to provide multiple copies of any information to the same person at the same time is met by providing a single electronic form of the information.

(4) A legal requirement to compare a document with an original may be satisfied by comparing that document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document.

4. Retention in electronic form

(1) Where any law requires certain documents, records, or information to be retained in paper or other non-electronic form, or provides for certain consequences if it is not retained in such form, that requirement is met by retaining it in electronic form if the following conditions are satisfied–

(a) the information contained in electronic form is accessible and usable for subsequent reference;

(b) the electronic record is retained in the format in which it was generated, sent, or received, or in a format which can be demonstrated to represent accurately the information generated, sent, or received; and

(c) any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received is retained.

(2) A person may satisfy the requirement under subsection (1) by using the services of any other person if the conditions set out therein are met.

5. Electronic time stamps.

(1) An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the ground that it is in an electronic form.

(2) An electronic time stamp shall be presumed accurate regarding the date and the time it indicates, and the integrity of the communication or data to which the date and time are bound, if it meets the following requirements:

(a) it binds the date and time to communication or data in such a manner as to reasonably preclude the possibility of the communication or data being changed without detection;

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using a digital signature, or advanced electronic seal, or by some equivalent method.

(3) The Regulatory Agency may develop rules, regulations, or guidelines for verifying the authenticity and integrity of electronic timestamps.

6. Delivery of information

(1) Subject to Section 44 of the Land Use Act, where any law requires information to be delivered, dispatched, given, sent, or served on a person, the requirement is met in doing so in the form of an electronic record.

(2) The form and means of delivery of the information under subsection (1) of this section must reliably ensure that the integrity of information contained in a document is maintained pursuant to section 37.

(3) Notwithstanding the provisions of subsection (1) of this section, where a law specifies a person to receive a piece of information, any information dispatched or delivered in accordance with this section shall be delivered or dispatched to the person specified under such law.

7. Other requirements

(1) Where a law requires a seal to be affixed to a document and the law does not prescribe the method or form by

which the document may be sealed, that requirement shall be met if the electronic record indicates that–

(a) it is required to be under seal and includes the digital signature of the person, or in the case of a body corporate, its authorised representative, as required by applicable law, by whom it is required to be sealed; or

(b) it is required to be under seal, and another type of electronic seal is used.

(2) Without prejudice to the Evidence Act, where a contract or deed requires any information, a signature, document or record to be notarised, apostilled, acknowledged, verified or made under oath, the requirement shall be satisfied if, in relation to an electronic signature or electronic record, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable law which shall also be construed to include their electronic format, is attached to or logically associated with the electronic signature or electronic record.

(3) Where the law requires payment to be made or issuance of any receipt of payment, that requirement shall be met if payment is made, or receipt is issued by an electronic means in accordance with any legislation relating to electronic payment.

(4) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print", "register" or words or expressions of similar effect, shall be interpreted to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

PART III – ELECTRONIC CONTRACTS

8. Formation and performance of contracts

(1) An offer, the acceptance of an offer, or any other matter that is material to the formation or performance of a contract may, unless the parties agree otherwise, or the law mandates the use

of a paper-based contract for transactions involving public institutions, be given by means of electronic communications.

(2) The electronic communication under subsection (1) of this section shall not be denied validity or enforceability solely on the ground that the contract was formed or performed with the use of electronic communication.

9. Use of automated systems for contract formation.

A commercial contract formed by the interaction of an automated system and an individual, or by the interaction of automated systems, shall, subject to the Nigeria Data Protection Act, not be denied validity or enforceability solely on the ground that no individual reviewed or intervened in each of the individual actions carried out by the automated systems or the resulting contract.

10. Error in electronic communications.

(1) Where an individual makes an input error in an electronic communication exchanged with the automated system of another party and the automated system does not provide the individual with an opportunity to correct the error, that individual, or the party on whose behalf that individual was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.

(2) The other party shall, in pursuance of subsection (1) of this section, maintain systems and processes that will enable the individual to, as soon as possible, exercise his right to withdraw the portion of the electronic communication in which the input error was made.

(3) The provisions of subsection (1) of this section shall not apply unless the individual, or the party on whose behalf that individual was acting–

(a) notifies the other party of the error as soon as reasonably practicable, after having learned of the error, and indicates that he made an error in the electronic communication; and

(b) has not used or received any material benefit or value from the goods or services received, if any, from the other party.

(4) Nothing in this section shall affect the application of any law that may govern the consequences of any error other than as provided for in sub-sections (1) and (2).

11. Invitation to make offer or treat.

A proposal made through one or more electronic communications, which –

(a) is not addressed to one or more specific parties;

(b) is generally accessible to parties making use of information systems; and

(c) invites the parties making use of the information system to make an offer;

shall be considered as an invitation to treat or make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

12. Intermediary liability.

(1) Notwithstanding anything contained in any law for the time being in force, but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third-party information, data, or communication, transmitted, stored, or hosted by it.

(2) The provisions of subsection (1) shall apply if –

(a) in the case of a mere conduit, the intermediary –

(i) does not initiate the transmission,

(ii) does not select the receiver of the transmission, and

(iii) does not select, create, or modify the information contained in the transmission;

(b) in the case of a provider of caching services, the intermediary –

(i) does not create or modify the information,

(ii) complies with conditions on access to the information established by the original source of the information,

(iii) ensures that the information is updated in accordance with globally recognised industry standards for information accuracy and maintenance,

(iv) does not interfere with the lawful use of technology, widely recognised and used by the relevant industry, to obtain data on the use of the information, and

(v) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement;

(c) in the case of a provider of hosting services, the intermediary –

(i) does not have actual knowledge of illegal activity or information and, in the case of claims for damages, is not aware of facts or circumstances that would make the illegal activity or information apparent; or

(ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

(d) the intermediary observes due diligence in observing all duly enacted laws and all subsidiary legislation to which it is subject.

(3) The provisions of subsection (1) shall not apply if –

(a) the intermediary has conspired or abetted or aided or induced the commission of the unlawful act; or

(b) upon receiving actual knowledge, or on being notified by the Regulatory Agency that any information, data, or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to the material on that resource without destroying evidence of the unlawful act.

13. Time and place of dispatch and receipt of electronic communications

(1) The time of dispatch of an electronic communication is, save as otherwise agreed between the originator and the addressee, presumed to be–

(a) the time when it leaves an information system under the control of the originator, or of the party who sent it on behalf of the originator; or

(b) if the originator and the addressee use the same information system, when it becomes capable of being retrieved and processed by the addressee.

(2) An electronic communication is, save as otherwise agreed between the originator and the addressee, presumed to be received by the addressee:

(a) if the addressee has designated or uses an information system for the purpose of receiving communications of the type sent, when it enters that information system and becomes capable of being retrieved and processed by the addressee; or

(b) if the addressee has not designated or does not use an information system for the purpose of receiving communications of the type sent, or if the addressee has designated or used such a system but the communication has been sent to another system, when the addressee becomes aware of the communication in the addressee's information system, and it becomes capable of being retrieved and processed by the addressee.

(3) Subject to section 6(1) of this Act, electronic communication shall, for the purposes of subsections (1) and (2) of this section, be deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.

(4) Subsections (2) and (3) shall apply notwithstanding that the location of the information system supporting an electronic address differs from the location where the

electronic communication is deemed received under subsection (2).

(5) For the purposes of this section —

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business; and

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

(6) The provision of this section shall not apply to any law regulating the payment of stamp duty in Nigeria insofar as it relates to a determination of the time of receipt in Nigeria of documents executed outside Nigeria.

14. Application of anti-competition and consumer protection rules

Nothing contained in this Part III shall be construed as exempting any person from compliance with the provisions of any anti-competition or consumer protection law pertaining to unfair business practices in the sale or supply of goods or services to the extent that such law does not derogate from the provisions of this Act, including sections 3,4,5,6,7,8,9,10,11, 12 and 13 of this Act.

PART IV – DIGITAL SIGNATURES

15. Legal recognition of electronic and digital signatures

An electronic and digital signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form.

16. Secured and reliable digital signature.

(1) Where a law requires that information or any other matter be authenticated by affixation of a signature, or that a document be signed or bear the signature of a person, such requirement shall be deemed to have been satisfied if the information or matter is authenticated by means of a digital

signature affixed in accordance with the provisions of this Act.

(2) A digital signature affixed in pursuance of subsection (1) shall be deemed secure, reliable, and to uphold integrity when the following requirements are met -

(a) it is unique to the person using it;

(b) it is capable of identifying the person using it;

(c) it is created in a manner or using a means under the sole control of the person using it;

(d) it is linked to the electronic record to which it relates in a manner such that if the record were changed, the digital signature would be invalidated; and

(e) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is reasonably detectable.

17. Certification of trust service providers

(1) A person shall not provide certified trust services unless the person is certified by the Regulatory Agency as a trust service provider under this Act.

(2) A trust service provider who, unless otherwise specified in this Act, provides certified trust services without obtaining certification from the Authority, commits an offence and is liable, upon conviction, to imprisonment for a term not exceeding 3 years, or a fine not exceeding ₦20,000,000, or both.

18. Affixation of digital signatures

A digital signature shall, for the purposes of section 16, be affixed on an electronic record using security infrastructure provided by a trust service provider certified in accordance with regulations or guidelines issued by the Regulatory Agency.

19. Presumptions as to digital signatures.

In any proceedings involving a digital signature affixed using security infrastructure from a trust service provider in accordance with regulations or guidelines issued by the Regulatory Agency, it shall, subject to the provisions of any law on admissibility, be presumed, unless evidence to the contrary is adduced, that–

(a) the digital signature is the signature of the person to whom it correlates;

(b) the digital signature was affixed by that person with the intention of signing or approving the electronic record; and

(c) the methods used by the security infrastructure to fulfil the requirements under this Part in relation to reliability, integrity, and security are appropriate.

20. Presumptions as to digital certificates.

In any proceedings involving a digital signature, it shall, subject to the provisions of any law on admissibility, be presumed, unless evidence to the contrary is adduced, that the information listed in a certificate issued in respect of a digital signature by the trust service provider is correct, if the certificate was accepted by the subscriber except for information specified as subscriber information which has not been verified.

21. Obligations of trust service providers

(1) A trust service provider issuing a certificate in respect of a digital signature shall—

(a) act in accordance with the representations made in its policies and practices;

(b) exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by it in relation to the certificate;

(c) provide reasonably accessible means for enabling the relying party to ascertain from the certificate -

(i) the identity of the trust service provider,

(ii) that the signatory identified in the certificate had control of the encrypted

signature creation device at the time when the certificate was issued,

(iii) that the encrypted signature creation device was valid and had not been compromised at the time when the certificate was issued,

(iv) the method used to identify the signatory,

(v) any limitation on the use, purpose, or value of the encrypted signature creation device or the certificate,

(vi) the existence of mechanisms and facilities for the signatory to give notice pursuant to section 26 (1)(b),

(vii) any limitation on the liability of the trust service provider, and

(viii) the procedures in place to effect revocation of the certificate issued by the trust service provider;

(d) utilise trustworthy systems, procedures, and human resources in performing its services; and

(e) comply with any other condition as may be prescribed by the Regulatory Agency.

(2) A trust service provider shall comply with privacy and data protection laws, including the Nigeria Data Protection Act.

(3) For the purposes of subsection (1) (d), in determining whether any systems, procedures, or human resources utilised by a trust service provider are trustworthy, regard may be had to –

(a) the provider's financial and human resources, including the existence of assets and the quality of their hardware and software systems;

(b) the provider's procedures for processing certificates and applications for certificates;

(c) the provider's retention of records and the availability of information to relying parties and to signatories identified in certificates;

(d) the regularity and extent of audits of the provider's operations by an independent body; and

(e) any other relevant factor as may be prescribed by the Regulatory Agency.

(4) A trust service provider who fails to comply with this section commits an offence and is liable, upon conviction, to imprisonment for a term not exceeding 2 years, or a fine not exceeding ₦10,000,000, or both.

22. Revocation and suspension of certificates

(1) A trust service provider may revoke or cancel a certificate issued in respect of a digital signature —
   (a) where the certificate was issued based on false, misleading, or fraudulent information;
   (b) where there has been a compromise or suspected compromise of the private key associated with the digital signature or seal;
   (c) upon the request of the certificate holder;
   (d) where the certificate holder has breached the terms and conditions under which the certificate was issued, including unauthorised or improper use; or
   (e) where a court order requires such revocation or cancellation.

(2) The trust service provider shall ensure that —
   (a) revocation or cancellation of a certificate is recorded on its website without delay; and
   (b) the certificate holder is notified without undue delay of the reason for the revocation or cancellation, and, where applicable, provided with an opportunity to appeal or request review, unless such disclosure would compromise ongoing investigations or pose security risks.

(3) A trust service provider may suspend a certificate temporarily pending investigation into any of the grounds under subsection (1) of this section, provided that such suspension is time-bound and followed by a final determination.

(4) Where a certificate is suspended under subsection (3) of this section, the trust service provider must, without delay, record the suspension, including its precise start and end date and time, on its website.

(5) A trust service provider shall not be liable for any loss or damage arising from a relying party's failure to check, or delay in checking, the up-to-date status of a certificate published on its website.

23. Liability of trust service providers

(1) Without prejudice to subsection (2) of this section, a trust service provider shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with section 21 of this Act.

(2) The intention or negligence of a trust service provider shall be presumed unless that trust service provider proves that the damage referred to in subsection (1) of this section occurred without the intention or negligence of that trust service provider.

(3) Where a trust service provider has duly informed a customer in advance of the limitations on the use of its services, or such limitations are reasonably apparent or capable of being identified by third parties, the provider shall not be liable for any damages arising from the use of the services beyond those stated limitations.

24. Recognition of foreign digital signatures and certificates.

(1) Subject to subsection (2) of this section, in determining the extent to which a digital signature or a certificate issued in any country other than Nigeria in respect of a digital signature is legally effective, no regard shall be given to the place where the digital signature or certificate was issued and the jurisdiction in which the issuer had its place of business.

(2) The provisions of subsection (1) of this section shall only be applicable to a digital signature, or the certificate issued thereof, that offers a substantially equivalent level of security and reliability in accordance with section 16 of this Act.

(3) For the avoidance of doubt, the recognition of foreign digital signatures or certificates under this section shall not be construed as conferring recognition or certification

upon the foreign entity or individual that issued such signatures or certificates.

25. Recognition of foreign trust service providers

(1) The certified trust services provided by a trust service provider established in a country outside Nigeria or an international organisation shall be recognised as legally equivalent to the services provided by a trust service provider certified under this Act, without the need for the foreign service provider to be certified locally under section 17 of this Act,

Provided that —

(a) the certified trust services originate from a country with which the Federal Republic of Nigeria has entered into a bilateral or multilateral agreement, memorandum of understanding, or international treaty governing mutual recognition of such services; and

(b) such recognition is consistent with applicable Nigerian laws and regulations on data protection and privacy.

(2) Any agreement referred to in subsection (1) shall provide that :

(a) the requirements applicable to trust service providers certified under this Act, including those relating to compliance with applicable data protection and privacy laws in Nigeria, are equivalently applied to and met by the trust service providers established in the third country or international organisation, and

(b) the certified trust services provided by the trust service providers under this Act are, in turn, recognised as legally equivalent to the services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

26. Obligations of the signatory.

(1) Where signature creation data or authentication data can be used to create a signature or authenticate any electronic record that has legal effect, each signatory shall–

(a) exercise reasonable care to avoid unauthorised use of its signature creation data or authentication data; and

(b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or provide services in support of the digital signature if–

(i) the signatory knows that the signature creation data or authentication data has been compromised;

(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data or authentication data may have been compromised; or

(c) where a certificate is used to support the digital signature or authentication data, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory, which are relevant to the certificate throughout its lifecycle, or which are to be included in the certificate.

(3) Where a signatory fails to notify relevant parties of a compromised signature creation or authentication data, the signatory shall first be issued a warning.

(4) If the failure to notify results in harm or is repeated, the signatory shall be deemed to have committed an offence and, upon conviction, shall be liable to imprisonment for a term not exceeding 6 months, or a fine not exceeding ₦1,000,000, or both.

(5) In cases of gross negligence or fraudulent behaviour, the signatory shall be deemed to have committed an offence and, upon conviction, shall be liable to imprisonment for a term not exceeding 3 years or a fine not exceeding ₦3,000,000 or both

PART V – ELECTRONIC TRANSFERABLE RECORDS

27. Legal requirement for transferable documents or instruments.

Where any law requires a transferable document or instrument, this requirement shall be met by an electronic record if–

(a) the electronic record contains the information that would be required to be contained in a transferable document or instrument; and

(b) in pursuance of section 36, a method that is reliable is used to–

(i) identify that electronic record as the electronic transferable record;

(ii) render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and

(iii) retain the integrity of that electronic record pursuant to section 37.

28. Control.

A person is deemed to have control of an electronic transferable record if the electronic transferable record is created, stored, and assigned in such a manner that:

(a) a single authoritative copy of the electronic transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (d), (e), and (f), unalterable;

(b) the authoritative copy identifies the person asserting control as:

(i) the person to whom the electronic transferable record was issued; or

(ii) if the authoritative copy indicates that the electronic transferable record has been transferred, the person to whom the record was most recently transferred;

(c) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(d) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(e) any version of the authoritative copy that is transmitted, retained, or otherwise made accessible, whether directly or indirectly, is clearly identifiable as a copy and not the authoritative version; and

(f) any revision of the authoritative copy is readily identifiable as authorised or unauthorised.

29. Indication of time and place in electronic transferable records.

Where a law requires or permits the indication of time or place with respect to a transferable document or instrument or provides for certain consequences if time or place is not indicated with respect to a transferable document or instrument, such requirement is satisfied if a reliable method pursuant to section 36, is used to indicate that time or place with respect to an electronic transferable record.

30. Endorsement

Where a law requires or permits the endorsement in any form of a transferable document or instrument, or provides for certain consequences if a transferable document or instrument is not endorsed, such a requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements set forth in sections 3 and 15.

31. Amendment

Where a law requires or permits the amendment of a transferable document or instrument or provides for certain consequences if a transferable document or instrument is not amended, such requirement is satisfied if a reliable method, pursuant to section 36, is used for the amendment of information in the electronic transferable record.

32. Presumption as to electronic transferable records

In any proceedings involving an electronic transferable record that is issued, transferred, controlled, presented and stored using security infrastructure provided by a trust service provider in accordance with regulations made by the Regulatory Agency, it is presumed, unless evidence to the contrary is adduced, that the

methods used by the security infrastructure to fulfil the requirements under this Part in relation to the electronic transferable record are as reliable as appropriate.

33. Replacement of a transferable document or instrument with an electronic transferable record.

(1) An electronic transferable record may replace a transferable document or instrument if, pursuant to section 36, a reliable method is used for the change of medium.

(2) For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the electronic transferable record.

(3) Upon issuance of the electronic transferable record in accordance with this section, the transferable document or instrument shall be made inoperative and shall cease to have any effect or validity.

(4) A change of medium in accordance with this section shall not affect the rights and obligations of the parties.

34. Replacement of an electronic transferable record with a transferable document or instrument.

(1) A transferable document or instrument may replace an electronic transferable record if–

(a) in pursuance of section 36, a reliable method used for the change of medium; and

(b) a statement indicating a change of medium is inserted in the transferable document or instrument.

(2) Upon issuance of the transferable document or instrument in accordance with this section, the electronic transferable record shall be made inoperative and shall cease to have any effect or validity.

(3) A change of medium in accordance with this section shall not affect the rights and obligations of the parties.

35. Recognition of foreign electronic transferable records

(1) Subject to subsection (2) of this section, in determining the extent to which an electronic transferable record is legally effective, no regard shall be given to the place where the electronic transferable record was issued and the jurisdiction in which the issuer had its place of business.

(2) The provisions of subsection (1) shall only be applicable to an electronic transferable record that offers a substantially equivalent level of reliability in accordance with the provisions of section 36 of this Act.

36. General reliability standard

For the purpose of this Part, a method shall be deemed reliable if it is–

(a) as reliable as is appropriate for the fulfilment of the function for which the method is being used, taking into consideration all relevant circumstances, including–

(i) any operational rules relevant to the assessment of reliability;

(ii) the assurance of data integrity;

(iii) the ability to prevent unauthorised access to and use of the system;

(iv) the security of hardware and software;

(v) the regularity and extent of audit by an independent body;

(vi) the existence of a declaration by the Regulatory Agency, an accreditation body or a voluntary scheme regarding the reliability of the method; or

(vii) any applicable industry standard; or

(b) proven in fact to have fulfilled the function by itself or together with further evidence.

37. Integrity of information

For the purposes of Parts I to V of this Act-

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the additions of any endorsement and any immaterial change which arises in the normal course of communication, storage and display; and
(b) the standard of integrity must be determined based on the purpose for which the information was generated and all the relevant circumstances.

38. Promotion of digital trade

(1) The Regulatory Agency shall, in collaboration with relevant public institutions, promote policies and programs that facilitate the growth of digital trade, cross-border e-commerce, and the participation of Nigerian businesses in the global digital economy.

(2) For the purpose of subsection (1), due regard shall be given to the provisions of applicable trade, commerce, and investment laws and international agreements to which Nigeria is a party.

39. Power to make regulations

The Board of the Regulatory Agency may make rules and regulations for carrying out the objectives of Parts I to V of this Act and, without prejudice to such general power, may make regulations for all or any of the following purposes –

(a) the regulation of trust service providers, including certification of trust service providers, security measures, auditing, and certificate issuance in respect of digital signature;
(b) safeguarding or maintaining the effectiveness and efficiency of the security infrastructure relating to the use of digital signatures and authentication of electronic records and digital time stamps;
(c) prescribing fees payable by trust service providers; and
(d) prescribing penalties, fines, or other corrective measures for failure to comply with the relevant provisions of the Act, rules, and regulations made thereto.

PART VI - CONSUMER PROTECTION, E.T.C.

40. Information to be provided

(1) Without prejudice to the Federal Competition and Consumer Protection Act, a supplier offering goods or services for sale, for hire, or for exchange by way of an electronic communication or transaction shall make the following information available to consumers on the website where such goods or services are offered:

(a) information about the supplier, including —

(i) full name or registered business name,

(ii) physical address,

(iii) website address, and

(iv) telephone number, e-mail address, and other means of prompt, easy, and effective consumer communication with the business;

(b) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction, including, as may be applicable —

(i) key functionality and interoperability features,

(ii) key technical or contractual requirements, limitations or conditions that may affect a consumer's ability to acquire, access, or use the good or service,

(iii) safety and health care information, and

(iv) any age restrictions;

(c) information relating to the transaction, including ——

(i) the full price of the goods or services, including transport costs, taxes, and any other fees or costs,

(ii) terms and conditions,

(iii) the manner of payment,

(iv) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored, and reproduced electronically by consumers,

(v) the time within which the goods will be dispatched or delivered or within which the services will be rendered,

(vi) the return, exchange, and refund policy of that supplier,

(vii) the security procedures and privacy policy of that supplier,

(viii) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently,

(ix) warranties and guarantees, and

(x) available dispute resolution and redress options, and a clear guide on how these may be accessed.

(2) The supplier must utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(3) The supplier is liable for any damage or loss suffered by a consumer due to a failure by the supplier to comply with subsections (1) and (2) of this section.

(4) A supplier intending to offer goods or services on an online platform shall, as a precondition for onboarding and activation of their account, be required to provide the information specified under subsection (1) of this section.

(5) An online platform shall not onboard or activate the account of any supplier who fails to provide the information required under subsection (1).

(6) A platform that contravenes this provision may be held jointly liable with the supplier for any damage or loss suffered by customers as a result of the supplier's non-compliance.

41. Unsolicited communications

(1) The transmission of unsolicited commercial communications to a consumer shall be permitted only in accordance with the Nigeria Data Protection Act, consumer protection laws, and relevant sector-specific laws in force.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

42. Redress mechanisms

(1) The provisions of the Federal Competition and Consumer Protection Act shall apply to the enforcement of any right of the

consumer under this Act, including any matter arising from a transaction, agreement, or dispute with a supplier of goods or services governed by this Act.

(2) Without prejudice to the Federal Competition and Consumer Protection Act, suppliers shall establish and maintain accessible, fair, and transparent internal complaints-handling procedures that enable consumers to raise and resolve complaints at the earliest possible stage and at no cost.

(3) Nothing in subsection (2) of this section shall be construed as requiring a consumer to utilise a supplier's internal complaints-handling mechanisms as a condition precedent to approaching the Commission.

CHAPTER THREE – DIGITAL GOVERNMENT

PART VII - INSTITUTIONAL FRAMEWORK FOR DIGITAL GOVERNMENT DEVELOPMENT

43. Objectives of digital government

The objectives of this Act with respect to digital government are to –

(a) ensure the adoption and integration of information technologies in public administration to streamline workflows, optimise data management, enhance public service delivery, and expand communication channels for citizen engagement and empowerment;

(b) promote the digital transformation of public services and institutions by leveraging advanced information and communication technologies as fundamental components of public administration;

(c) enhance public access to government information, such as to foster transparency and accountability within public institutions;

(d) ensure a framework for the continuous improvement of digital government initiatives, ensuring the adoption of best-in-class technologies;

(e) ensure the continuous development and maintenance of the necessary infrastructure to support digital government initiatives; and

(f) centralise digital government strategies and policies to ensure consistency, efficiency, and effective implementation across all levels of government.

44. National digital government strategy

(1) The Minister, in consultation with the Head of Civil Service of the Federation, public and private institutions, as the Minister deems necessary, shall, within 12 months of the commencement date of this Act, develop a digital government strategy framework in accordance with international good practices and the provisions of this Act.

(2) The digital government strategy framework under subsection (1) of this section shall, at a minimum, include:

(a) a detailed roadmap for the digitalisation of government processes and adoption of e-government initiatives, including specific goals, timelines, and milestones;

(b) strategies for developing and implementing a national broadband plan to ensure widespread, reliable, and high-speed internet access across Nigeria, essential for the success of digital government initiatives;

(c) strategies to minimise the paper-based processes within public bodies, promoting digital record-keeping and electronic workflows;

(d) strategies for efficient management and secure handling of administrative information resources by public institutions;

(e) plans for gradually providing services through electronic means, with a view to progressively reducing the need for human-to-human interaction, enhancing efficiency and convenience for citizens;

(f) defined phases for implementing the provisions of this Act and the digital government strategy framework, including specific deadlines, transition periods, standards, and performance benchmarks;

(g) identification of priority areas for the implementation of digital government programs, with a focus on key sectors critical to national development;

(h) projects for establishing and maintaining a robust information and communications network among public institutions that ensure security and reliability;
(i) initiatives to foster the harmonisation and integration of digital systems among public institutions, promoting interoperability and integrated services;
(j) development and maintenance of a single, unified portal for all government-related services, such as providing a streamlined and user-friendly experience for citizens;
(k) comprehensive medium and long-term plans for digital government projects, detailing strategies for sustainable development and continuous improvement;
(l) frameworks for establishing long-term public-private partnerships to support the development, implementation, and maintenance of digital government projects;
(m) initiatives to ensure the security, privacy, and protection of data within all digital government systems;
(n) strategies to ensure all digital government services are accessible in multiple languages, including major Nigerian languages, and are designed to be inclusive for all citizens, including those with disabilities;
(o) mechanisms to ensure public participation, feedback, and continuous improvement in the development and implementation of digital government initiatives;
(p) measures to ensure the integrity, reliability, and minimal downtime of digital government systems, including regular maintenance schedules and contingency plans for system failures;
(q) strategies for ensuring the effective implementation of this Act within public institutions; and
(r) any other information as may be deemed necessary by the Minister to ensure the effective implementation and operation of digital government initiatives.

(3) The Minister shall ensure that the digital government strategy is reviewed on an annual basis.

(4) Every public institution shall, in preparing its estimates of revenues and expenditure for the budgetary process, ensure that such estimates, as is reasonably practicable, make provisions for the

implementation of the strategies, initiatives, and projects outlined in the digital government strategy framework.

(5) The President shall, where the estimates of revenues and expenditure to be laid before the National Assembly do not make provision for the implementation of the digital government strategy framework, require the amendment of such estimates of revenues and expenditure to align with the framework before submitting them to the National Assembly.

PART VIII- DIGITAL GOVERNMENT SYSTEMS AND SERVICES

45. Institutional ICT Unit

(1) Every public institution shall establish and maintain an ICT Unit adequately staffed with qualified personnel to support the institution's information security and digital service delivery objectives.

(2) The specific minimum qualifications and experience for ICT Unit personnel shall be prescribed by the Regulatory Agency by regulation in consultation with the Head of Civil Service of the Federation.

(3) The ICT Unit shall be responsible for—

(a) supporting the institution's operational efficiency and delivery of digital government services;

(b) providing strategic input and technical oversight on all ICT security matters;

(c) monitoring ICT systems to ensure compliance with the institution's ICT security policies and applicable regulatory standards;

(d) performing regular vulnerability assessments and penetration testing, as may be prescribed by the Regulatory Agency;

(e) securing institutional networks through appropriate segmentation and the deployment of intrusion detection and prevention mechanisms;

(f) applying timely updates and security patches to protect against known vulnerabilities in operating systems and application software;

(g) conducting security testing prior to the deployment of critical applications;
(h) protecting institutional data from unauthorised interception, alteration, or destruction, whether at rest, in transit, or during processing;
(i) implementing and maintaining endpoint security measures for all ICT equipment in accordance with standards prescribed by the Regulatory Agency;
(j) monitoring ICT systems to detect anomalies, breaches, or other security incidents;
(k) implementing appropriate incident response procedures, including containment, investigation, recovery, and post-incident review, in accordance with standards prescribed by the Regulatory Agency; and
(l) perform any other function as may be prescribed by the Regulatory Agency.

46. Nigeria Data Exchange

(1) There is established a Nigeria Data Exchange (NDE), to serve as the secure platform for information exchange among all government databases, registries, and digital systems.

(2) The objectives of the NDE shall be to—
(a) ensure interoperability and seamless data sharing across government systems and agencies;
(b) guarantee data integrity, confidentiality, and availability in line with the Nigeria Data Protection Act and other applicable laws;
(c) enable trusted services, including timestamping, audit trails, secure logging, identity verification, encryption, and authentication of all data transactions;
(d) provide a unified and cost-efficient platform that reduces duplication of infrastructure and promotes transparency, accountability, and efficiency in public service delivery; and

(e) ensure that all data exchange activities are consistent with best-practice governance, cybersecurity, and data protection frameworks in Nigeria.

(3) The NDE shall operate within the shared data infrastructure of the Federal Government and shall be hosted within infrastructure that is fully or partly owned by the Federal Government, under the oversight of the Minister in consultation with relevant public institutions.

(4) The Minister shall, in consultation with relevant stakeholders, issue regulations, guidelines, and technical frameworks for the governance, operation, and security of the NDE, including data standards, metadata requirements, and access protocols.

(5) All public institutions operating digital infrastructure shall—

(a) integrate their systems with the NDE within the timeline prescribed by the Minister;

(b) ensure that all inter-agency data exchanges occur exclusively through the NDE; and

(c) comply with the minimum interoperability, cybersecurity, and data protection standards issued by the Minister.

(6) For the purpose of this Act, the shared data infrastructure of government shall mean the infrastructure of the Federal Government that is operated within a fully or partly owned facility of the Federal Government, as may be designated by the Minister.

47. Digital government infrastructure

(1) Public institutions shall, for the purpose of ensuring the effective and sustainable optimisation of government digital infrastructure, submit the design and implementation plan for any digital technology project that exceeds the financial or technical thresholds set from time to time by the Regulatory Agency, in consultation with the Bureau of Public Procurement, for review and approval by the Regulatory Agency prior to implementation.

(2) The Regulatory Agency shall make regulations, guidelines, and other subsidiary legislation for the planning, deployment, optimisation, and security of digital infrastructure, including in relation to digital public infrastructure and public key

infrastructure, pursuant to its mandate under the National Information Technology Development Agency Act.

(3) All digital infrastructure adopted or operated by public institutions shall conform to the minimum standards, specifications, and operational procedures prescribed by the Regulatory Agency for the purposes of ensuring interoperability, security, and efficiency in public service delivery.

(4) For the purpose of ensuring cost-effectiveness and information and communication technologies readiness, construction of any government-owned infrastructure, including roads, railways, buildings, fibre cables and such other infrastructure shall, subject to the guidelines issued by the relevant authorities, include information and communication technologies infrastructure as part of the project design in accordance with the appropriate regulation issued by the Regulatory Agency.

48. Service Level Agreements for digital technology services

(1) Any person or public institution that intends to provide digital technology services to, or on behalf of, a public institution within the digital economy shall do so pursuant to a written service level agreement.

(2) The service level agreement shall, at a minimum, contain –

(a) scope of services, technical specifications, quality benchmarks, delivery timelines, and performance indicators;

(b) compliance with technical, operational, and security standards prescribed by the Regulatory Agency; and

(c) system availability, including uptime guarantees, maintenance obligations, auditability, data handling procedures, incident response protocols, and remedies in the event of non-performance or breach.

(3) The Regulatory Agency shall, in consultation with relevant sector regulators and recognised standards organisations, prescribe mandatory technical standards and model service level agreements applicable to public sector digital services and infrastructure.

(4) The standards under subsection (3) shall address, at a minimum –

(a) interoperability;

(b) cybersecurity data resilience, and threat mitigation;

(c) data integrity and protection;
(d) service continuity, disaster recovery, and failover mechanisms; and
(e) user accessibility and inclusion.

(5) No public institution shall enter into any contract or procurement arrangement for the provision of digital technology services unless it includes a service level agreement that complies with the requirements set out in this section.

49. Electronic communication of government

(1) All public institutions shall establish and maintain effective communication channels to ensure seamless service delivery to the public.

(2) The Regulatory Agency shall, for the purpose of subsection (1) of this section, prescribe –
(a) the standards for systems and devices approved for official government communication;
(b) the categories, types, and classifications of information and data that may be transmitted via electronic communication, without prejudice to any law governing the classification of official government information; and
(c) the categories, types, and classifications of information and data that are prohibited from being transmitted through electronic communication.

50. Services provided by public institutions

(1) Every public institution shall, subject to section 44 (2) (f) of this Act –
(a) use digital technologies to enable the provision of administrative processes;
(b) address organisational, legal, and technological requirements necessary to enhance digital service delivery and interoperability; and
(c) develop and implement plans to establish and improve systems for digital government services within the timeline prescribed in the national digital government strategy.

(2) Where a public institution does not comply with subsection (1) of this section or fails to implement the remedial actions directed by

the Regulatory Agency under section 51(2), the Minister may recommend to the President such corrective actions, which may include –

(a) suspension of certain administrative privileges where such privileges are enabling the non-adoption of digital solutions by that public institution;

(b) restriction to specific funding, where the utilisation of such funds will hinder the adoption of digital solutions; and

(c) mandatory restructuring or reorganisation to address the identified deficiencies.

(3) All public institutions shall ensure that their activities, processes, and procedures are aligned with the national digital government strategy framework.

51. Digital Maturity and Readiness Assessments

(1) All public institutions shall be subject to periodic digital maturity and readiness assessments by the Regulatory Agency to evaluate their level of preparedness, capability, and performance in implementing the national digital government strategy framework and the provisions of Part VIII of this Act.

(2) The Regulatory Agency shall, where an assessment reveals gaps, deficiencies, or non-compliance with the provisions of Part VIII of this Act, or the national digital government strategy framework, notify the public institution in writing, stating the —

(a) findings of the assessment;

(b) action required to remedy the gaps or deficiencies; and

(c) period within which a public institution shall take the remedial action.

(3) Where a public institution fails to comply with the remedial actions issued by the Regulatory Agency within 30 days or such other period as may be prescribed by the Regulatory Agency, the Agency shall recommend to the Minister the imposition of corrective measures as provided under section 50(2) of this Act.

52. Principles for effective delivery of digital government services

(1) All public institutions shall ensure that digital government services –

(a) are accessible to all users, regardless of age, ability, language proficiency, or socio-economic status, and are designed to meet user needs in an efficient and effective manner;

(b) are affordable, ensuring that users can access digital government services without undue financial burden;

(c) maintain the highest security standards to protect against cyber threats, ensure privacy, and safeguard sensitive information;

(d) deliver consistent, high-quality services, with clear performance standards, and impose penalties for failure to meet those standards;

(e) include robust feedback mechanisms that allow users to voice concerns and make suggestions;

(f) are designed, developed and delivered in accordance with digital public infrastructure standards issued by the Regulatory Authority; and

(g) align with the national digital strategy, with mandatory periodic digital maturity and readiness assessments to ensure compliance.

(2) Public institutions shall be required to adhere to these principles in the design, implementation, and operation of digital government services.

(3) The Regulatory Agency shall oversee the enforcement of these principles and ensure that institutions are held accountable for non-compliance.

53. Creation and use of an electronic gazette

(1) The Federal Government Printer shall establish and maintain an electronic gazette as the official platform for the publication of documents mandated to be published in a gazette, in Nigeria.

(2) The electronic gazette shall -

(a) provide easy access to all published documents, with features for regular updates, search functionality, and efficient retrieval to promote transparency and public access.

(b) be considered an official medium for fulfilling legal publication requirements.

(c) have the same legal standing as a printed Gazette, and its contents shall be deemed legally binding from the date of publication.

(3) The date of publication in the electronic gazette shall be regarded as the official date for all legal purposes requiring a date of publication in a gazette.

(4) The Electronic Gazette shall be fully operational within 12 months from the commencement of this Act.

54. Public institutions' responsibility for digital government implementation

(1) A public institution shall ensure that the digital government initiatives of the institution are managed in compliance with guidelines issued by the Regulatory Agency.

(2) A public institution shall conduct, on an annual basis, a self-assessment on the implementation of digital government initiatives by the institution.

(3) The self-assessment under subsection (1) of this section shall be completed no later than the end of the preceding financial year.

(4) A self-assessment report under this section shall be submitted to the Regulatory Agency on demand.

(5) Public officers, in addition to other requirements for promotion, shall obtain appropriate digital literacy certification relevant to their cadre, as may be specified by the Federal Civil Service Commission in consultation with the Regulatory Agency.

(6) For the purpose of subsection (5), the Federal Civil Service Commission and the Regulatory Agency shall take into account the National Digital Skills Development Framework under Section 56 of this Act.

(7) A public institution shall comply with privacy and data protection laws, including the Nigeria Data Protection Act.

55. Regulations under Parts VII-VIII

(1) The Board of the Regulatory Agency shall have the authority to issue regulations, guidelines in consultation with the Office

of the Head of Civil Service of the Federation, or directives to enforce compliance with the provisions of Part VII-VIII of this Act.

(2) The regulations, guidelines, or directives issued by the Regulatory Agency may cover, but are not limited to:

(a) establishing technical and procedural standards for the development, management, and delivery of digital government services; and

(b) procedures for monitoring and evaluating adherence to the provisions of this Act, including regular audits and assessments.

(3) The Board of the Regulatory Agency shall periodically review the effectiveness of the regulations and make amendments as necessary to address emerging issues, technological advancements, and changes in good practices.

PART IX: NATIONAL DIGITAL SKILLS DEVELOPMENT FRAMEWORK E.T.C.

56. National Digital Skills Development Framework

(1) The Minister shall, in consultation with the Minister responsible for education, establish a National Digital Skills Development Framework (the "Framework") to ensure a harmonised and strategic approach to the planning, design, implementation, and oversight of digital literacy and skills acquisition initiatives across the public sector, and public and private educational institutions.

(2) The Framework shall, at a minimum —

(a) prescribe minimum digital literacy standards and competency benchmarks for integration into—

(i) formal education curricula at the basic, secondary, tertiary, and vocational levels;

(ii) public service entry-level and in-service training programmes;

(iii) workforce development and reskilling initiatives;

(b) establish standards and certification requirements for the accreditation and continuous professional development of digital literacy trainers and facilitators;

(c) provide for the integration of digital competence modules in national curricula, with particular emphasis on foundational skills, safe and ethical use of digital technologies, and critical thinking in digital environments;
(d) promote equity and inclusion by identifying and addressing digital skills disparities affecting underrepresented or marginalised groups, including women, persons with disabilities, youth, and rural or remote populations;
(e) provide mechanisms for inter-agency coordination, public-private partnerships, and periodic evaluation to ensure that digital skills initiatives remain current, accessible, and aligned with evolving technological trends and labour market needs.

57. Private sector participation and non-tax incentives

(1) The President shall encourage private sector involvement in digital workforce development by —

(a) facilitating public-private partnerships (PPPs) for digital skills training, apprenticeships, and internship programs;

(b) recognising private and community-led digital training providers that are certified by relevant regulatory authorities in national programs and funding initiatives;

(c)providing non-tax incentives, including—

(i) preferential access to government-sponsored innovation challenges or public contracts;

(ii) recognition and award schemes for top-performing training organisations; and

(iii) support with infrastructure, including broadband access, training equipment in underserved regions.

58. Recognition of non-traditional certifications

For purposes of public employment, skills accreditation, and government-funded training programs, all public institutions shall:

(a) recognise alternative and non-traditional certifications, including bootcamp diplomas, online course

completions, micro-credentials, and industry-recognised badges issued by reputable digital platforms; and

(b) ensure that digital competence is evaluated based on demonstrable skills and practical knowledge rather than solely on formal academic qualifications.

59. Implementation and monitoring

(1) The Regulatory Agency, in collaboration with the National Universities Commission, the National Board for Technical Education, and relevant professional bodies, shall—

(a) develop modules, programmes, and hold workshops aimed at imparting knowledge on digital technology;

(b) establish a digital skills registry and reporting framework to track training delivery, learner outcomes, and market demand alignment; and

(c) promote the provision of information infrastructure linking research institutions to facilitate cooperation and sharing of research information and knowledge.

(2) The Regulatory Agency shall, in collaboration with relevant private and public institutions, develop and publish an annual Digital Workforce and Skills Development Report, which shall be submitted to the Minister for approval prior to its publication.

(3) The Digital Workforce and Skills Development Report under subsection (2) of this Section shall assess the status, investments, gaps, and opportunities within the digital workforce in Nigeria.

CHAPTER FOUR – CYBERSECURITY TRUST, AND INFORMATION SECURITY

PART X- COMPLIANCE WITH CYBERSECURITY LAWS AND INFORMATION SYSTEM SECURITY

60. Compliance with cybersecurity laws

All persons and public institutions subject to this Act shall comply with all applicable cybersecurity laws, regulations, and directives, including the Cybercrime (Prohibition, Prevention, etc.) Act, 2015,

and any cybersecurity standards or frameworks issued under applicable law.

61. Coordination and enforcement

The Office of the National Security Adviser, with technical support from the National Cybersecurity Coordination Centre and in consultation with the Regulatory Agency, shall —

(a) promote awareness and digital literacy relating to cybersecurity among citizens and micro, small, and medium enterprises;

(b) encourage innovation in indigenous cybersecurity solutions, including support for local startups and research initiatives; and

(c) integrate cybersecurity risk assessment, prevention, and response mechanisms into e-Government platforms and national digital systems.

62. Public institution information system security

(1) Every public institution shall, in accordance with information security standards issued by the Regulatory Agency, implement and maintain appropriate measures to ensure the confidentiality, security, integrity, and availability of information processed in connection with digital government services.

(2) Without prejudice to subsection (1) of this section, each public institution shall—

(a) develop, implement, and enforce an ICT security policy and strategy to prevent unauthorised access, disclosure, alteration, or destruction of information;

(b) take reasonable steps to ensure that all officers involved in the provision, collection, management, publication, or dissemination of digital services or information are aware of, and comply with, applicable ICT security measures;

(c) establish and maintain an information system continuity management framework, which shall include—

(i) implementing secure backup and restoration mechanisms for ICT system continuity;

(ii) developing and maintaining a disaster recovery plan; and

(iii) conducting periodic testing of the disaster recovery plan as may be prescribed by the Regulatory Agency, and submitting test reports accordingly;

(d) conduct regular ICT security risk assessments at intervals specified by the Regulatory Agency;

(e) prepare and submit ICT security reports to the Regulatory Agency in the format and frequency it may require; and

(f) cooperate with the Office of the National Security Adviser, National Computer Emergency Response Team Coordination Center, Sectoral Computer Emergency Response Teams, Sectoral Security Operation Centres, and other relevant cybersecurity authorities in matters related to cyber threat intelligence, incident response, and critical infrastructure protection.

CHAPTER FIVE – REGULATION OF ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES

PART XI - ETHICAL GOVERNANCE OF ARTIFICIAL INTELLIGENCE

63. Principles for artificial intelligence development and application

(1) Any person or public institution that develops, deploys, or uses an artificial intelligence system shall ensure that—

(a) The system is fair, inclusive, and non-discriminatory, and is designed and implemented in a manner that prevents the reinforcement or amplification of existing biases or unlawful discrimination;

(b) the system is transparent, explainable, intelligible, and traceable, supported by documentation and technical measures that enable understanding of its functioning, rationale, and decision-making processes;

(c) the system is safe, secure, and robust, ensuring reliable performance and minimising risks of harm or failure;
(d) responsibility for the system's operation and outcomes is assigned to a specific individual or entity, who can be held accountable;
(e) the system incorporates mechanisms for due process, including contestability of decisions, and provides access to effective remedies and redress for harms caused;
(f) the system is subject to meaningful human oversight, ensuring that its design, deployment, and use remain under the direction and control of competent individuals; and
(g) the system complies with all applicable laws and regulations, including the Nigeria Data Protection Act.

(2) The Regulatory Agency may, by regulation, amend, alter, revise, or expand the principles in subsection (1).

64. Obligations of artificial intelligence agents

(1) An artificial intelligence agent shall –
(a) implement governance, risk management, and impact assessment measures that are proportionate to the nature, classification, and risk level of the artificial intelligence system;
(b) promote the design, development, and use of artificial intelligence systems that are inclusive and accessible;
(c) provide users and affected persons with clear, accurate, sufficient, and accessible information about the system's function, limitations, and potential impacts;
(d) adopt safeguards to detect and reduce discriminatory outcomes, including indirect bias, and mitigate risks to privacy and to the physical, psychological, and moral well-being of individuals;
(e) design and operate systems to function reliably, safely, and with sufficient resilience to minimise the risk of harm or malfunction;
(f) maintain documentation and records sufficient to enable independent oversight, auditing, and traceability of the system's outputs, aligned with its complexity and risk profile;

(g) disclose, in a transparent and accessible manner, the identity and contact information of the provider or operator responsible for the system, for purposes of inquiry, redress, or the exercise of legal rights;
(h) allow for human oversight or intervention in the operation of artificial intelligence systems when their use may cause significant risks to the rights of affected persons;
(i) ensure that the systems are used in accordance with good practices of information security and protection of personal data;
(j) cooperate with the Regulatory Agency and the Nigeria Data Protection Commission to ensure compliance with this Act and applicable data protection laws; and
(k) comply with other responsibilities as may be prescribed by the Regulatory Agency in a regulation.

(2) The obligations under subsection (1) of this section shall be fulfilled in a manner compatible with the level of risk associated with the artificial intelligence system, its stage of development or implementation, and the technical and economic capacity of the artificial intelligence agent.

65. Classification of artificial intelligence

(1) The Regulatory Agency may, with the approval of the Minister, by regulation, classify artificial intelligence based on risk levels, taking into account —
(a) the purpose and context of the use of the system;
(b) the nature, scope, and extent of its application;
(c) the likelihood and severity of damages and impacts that may result from the use of the system;
(d) the reversibility of the effects of the system on the rights of affected persons;
(e) the degree of autonomy of the system and the possibility of human oversight or intervention;
(f) the level of control exercised by the artificial intelligence agent over the functioning and outcomes of the system;

(g) the capacity of the artificial intelligence agent to mitigate risks and provide safeguards; and
(h) the population groups or social segments that are affected, particularly vulnerable groups.

(2) The classification made under subsection (1) shall guide the Regulatory Agency in allocating responsibilities and determining regulatory measures, ensuring that the obligations imposed on artificial intelligence agents correspond proportionately to the risk level of each classified artificial intelligence system.

66. Regulatory Agency functions in respect of artificial intelligence systems

The Regulatory Agency shall —

(a) be responsible for monitoring and ensuring compliance with the provisions of this Part of the Act;
(b) assess and monitor risks across the Federal Republic of Nigeria arising from artificial intelligence systems;
(c) conduct horizon-scanning, including by consulting the artificial intelligence industry, to inform a coherent response to emerging artificial intelligence system technology trends;
(d) accredit independent artificial intelligence system auditors;
(e) conduct inspections, audits, and investigations to verify compliance with this Act and regulations issued thereto;
(f) impose sanctions or take enforcement action, where necessary, in accordance with this Act;
(g) promote public education and awareness regarding the risks, benefits, and responsible use of artificial intelligence;
(h) support capacity-building and training initiatives for stakeholders involved in the artificial intelligence lifecycle;
(i) facilitate technical collaboration to support the responsible, secure, and ethical development, deployment, and use of artificial intelligence systems;

(j) support testbeds and sandbox initiatives to help artificial intelligence system innovators get new technologies to market; and
(k) do anything which, in the opinion of the Regulatory Agency, is incidental or ancillary to its functions under this Part of the Act.

67. Regulatory Agency powers in respect of artificial intelligence systems

In the exercise of its functions under this Part of the Act, the Regulatory Agency may —
(a) request information, documents, and clarifications from artificial intelligence agents and other relevant parties;
(b) issue warnings or recommendations to any artificial intelligence agent;
(c) promote or require audits and impact assessments related to artificial intelligence systems;
(d) determine the adoption of corrective measures or the suspension of activities involving artificial intelligence systems that pose imminent or serious risks;
(e) impose administrative sanctions for non-compliance with this Act; and
(f) issue any regulation, rule, or other subsidiary legislation for the safe, ethical, and lawful development and use of artificial intelligence systems or to give effect to this Part of the Act.

68. Enforcement Order

(1) Where the Regulatory Agency, after an investigation, is satisfied that an artificial intelligence agent has violated any provision of this Act, or any regulation, rule, or other subsidiary legislation made thereunder, it may make any appropriate enforcement order or impose a sanction on the artificial intelligence agent.
(2) An enforcement order made, or a sanction imposed under subsection (1), may include the following—
    (a) requiring the artificial intelligence agent to remedy the violation;

(b) ordering the artificial intelligence agent to pay compensation to an affected person who suffers injury, loss, or harm as a result of a violation;
(c) ordering the artificial intelligence agent to account for the profits made out of the violation; or
(d) ordering the artificial intelligence agent to pay a penalty not exceeding the higher of ₦10,000,000, and two percent of its annual gross revenue derived from Nigeria in the preceding financial year.

(3) Artificial intelligence agents shall be civilly liable for material and moral damages as may be determined by the court caused by the development, implementation, or use of artificial intelligence systems.

69. Annual system impact assessment report on AI systems

The Minister shall, based on the recommendation of the Regulatory Agency, publish an annual system impact assessment report, which shall evaluate compliance with applicable standards, assess the sectoral impacts of such technologies, and provide recommendations for legal, technical, and policy improvements

PART XII - REGULATORY SANDBOXES AND TESTBEDS FOR ARTIFICIAL INTELLIGENCE

70. Regulatory sandboxes and testbeds

The Regulatory Agency shall, in collaboration with relevant sectoral regulators, establish and administer a framework for the controlled testing and supervision of artificial intelligence systems through regulatory sandboxes and operational testbeds.

71. Guiding considerations for regulatory sandboxes and testbeds

In developing the framework for regulatory sandboxes and testbeds, the Regulatory Agency shall be guided by the following considerations —

(a) need to support responsible innovation and enable the safe, controlled introduction of artificial intelligence technologies into the market;
(b) the importance of identifying potential regulatory gaps, risks, and sectoral impacts at an early stage in the development and deployment lifecycle of artificial intelligence systems;
(c) the importance of enabling the continuous improvement and refinement of artificial intelligence systems, subject to appropriate safeguards and regulatory oversight;
(d) the promotion of collaboration between technology developers, regulators, researchers, users, and affected stakeholders in the testing process;
(e) the goal of ensuring that artificial intelligence systems meet baseline standards of safety, fairness, transparency, privacy, and accountability before broader deployment or commercialisation.

72. Inter-Agency collaboration for regulatory sandboxes and testbeds

The Regulatory Agency may make regulations prescribing the structure, governance, and inter-agency coordination mechanisms for the implementation of regulatory sandboxes and testbeds under this Part of this Act.

73. Eligibility and prioritisation for participation

In administering the regulatory sandbox or testbed, the Regulatory Agency shall establish eligibility requirements and shall prioritise—

(a) applicants that are Nigerian-registered startups, macro, small, and medium-sized enterprises, or ventures with significant local ownership or operations;
(b) applicants that demonstrate the use or development of proprietary technology, locally conducted research and development, or make active contributions to technical capacity building within Nigeria;
(c) applicants that target underserved or marginalised populations, including women, youth, persons with

disabilities, or rural communities, or focus on addressing domestic challenges in sectors such as healthcare, agriculture, education, financial inclusion, public infrastructure, or climate resilience; or

(d) applicants with proposed innovations that show potential for broader application, scalability, or contribution to local or regional markets.

74. Grant of regulatory flexibility status

(1) An entity participating in an innovation sandbox or testbed under this Act may be granted a regulatory flexibility status by the Regulatory Agency, subject to terms and conditions prescribed by regulation.

(2) The regulatory flexibility status may enable the temporary testing or validation of innovative products, services, or systems under adjusted or relaxed regulatory conditions, and shall be subject to the following conditions –

(a) it may allow limited exemptions or modifications from specific regulatory requirements, provided that the entity maintains compliance with fundamental obligations relating to safety, data protection, consumer rights, and national security;

(b) it shall be granted for a clearly defined duration, not exceeding the testing period, after which the entity must either transition to full regulatory compliance, apply for appropriate authorisation, or discontinue its activities within the sandbox or testbed; and

(c) it shall be issued for a fixed and pre-determined duration corresponding to the testing or experimental phase, which shall not exceed the maximum period specified by the Regulatory Agency, after which the entity shall—

(i) apply for full regulatory authorisation, licence, or registration in accordance with applicable law,

(ii) transition to full compliance with the regulatory framework, or

(iii) cease all activities conducted under the sandbox or testbed;

(d) it shall be governed by a clear and transparent framework, including defined eligibility criteria, application and selection procedures, testing plans, performance metrics, risk mitigation measures, and exit strategies, to be issued by the Regulatory Agency in consultation with relevant sectoral regulators.

(3) The grant of regulatory flexibility shall not compromise the overarching goals of ethical innovation, public trust, and legal accountability in the deployment of artificial intelligence systems.

75. Outcomes and integration into regulatory and policy frameworks

(1) Where an entity successfully completes participation in a testbed or innovation sandbox under this Act, the Regulatory Agency may, subject to guidelines issued pursuant to this Act —

(a) facilitate the entity's transition into the full regulatory regime through streamlined licensing or approval processes; and

(b) recognise the results of the testbed or sandbox process as evidence of compliance with applicable regulatory requirements, where appropriate.

(2) The outcomes and insights derived from testbed and sandbox activities shall—

(a) be documented in the annual system impact assessment report under section 69 of this Act;

(b) inform the periodic review and amendment of applicable national regulatory, legal, and policy frameworks governing artificial intelligence systems; and

(c) be disseminated to relevant government agencies and bodies to support coordinated approaches to innovation, oversight, and risk management.

76. Supervision and risk controls

(1) All entities admitted into a regulatory sandbox or testbed pursuant to this Act shall be subject to continuous

oversight by the Regulatory Agency and shall comply with applicable risk control measures and reporting obligations.

(2) Each participant shall—

(a) implement and maintain appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of systems, including compliance with applicable data protection, cybersecurity, and consumer protection laws;

(b) submit periodic reports, in the form and frequency prescribed by the Regulatory Agency, which shall include, at a minimum—

(i) updates on the operational performance and testing outcomes of the product, service, or system under evaluation;

(ii) identification of any emerging risks or incidents, including those affecting users or the broader ecosystem;

(iii) a description of user feedback, complaints, and any corrective measures implemented; and

(iv) an assessment of the innovation's potential for scale, impact, and regulatory compliance;

(c) ensure that the testing and deployment of any product, service, or process does not result in material harm, deception, disruption, or financial loss to participating users, consumers, or members of the public;

(d) comply with other compliance requirements imposed by the Regulatory Agency by a regulation, in consultation with relevant sectoral regulators.

(3) The Regulatory Agency may, in consultation with relevant sectoral regulators, make rules, regulations, and other subsidiary legislation for carrying out the objectives of this Part of the Act.

77. Revocation of sandbox or testbed participation

(1) The Regulatory Agency may suspend, limit, or revoke a participant's regulatory flexibility status, and require the

immediate cessation of any activity conducted within the sandbox or testbed, where—

(a) the participant fails to comply with applicable laws, regulations, or conditions of participation;

(b) the activity or system under testing poses or is likely to pose a material risk to individual rights, market stability, public health, safety, national security, or the environment;

(c) the participant fails to demonstrate adequate progress, innovation viability, or readiness for regulatory transition within the designated period; or

(d) any misrepresentation, concealment of material facts, or misuse of the sandbox or testbed framework is established.

(2) The decision of the Regulatory Agency to revoke or suspend regulatory flexibility status shall be communicated in writing to the affected entity, stating the grounds for such action and affording the entity an opportunity to respond.

78. Regulation of emerging technologies

(1) The Federal Government shall establish a regulatory framework for the development, deployment, and use of emerging technologies other than artificial intelligence.

(2) The framework shall provide for—

(a) the development and implementation of resistant cryptographic protocols to secure digital infrastructure and national security;

(b) the establishment of ethical and technical standards for their research and applications; and

(c) international cooperation and strategic partnerships that enable Nigeria's participation in the global emerging technologies economy, with measures to protect national interests and technological sovereignty.

79. Procurement for innovation sandbox services in the public sector

The Regulatory Agency shall, in collaboration with the Bureau of Public Procurement, issue regulations, guidelines, or other subsidiary legislation governing the procurement of service providers and technology solutions deployed within innovation sandboxes in the public sector.

CHAPTER SIX – GENERAL PROVISIONS

Part XIII- PROMOTION OF INNOVATION, AND MINISTER'S DIRECTIVES

80. Promotion of local innovation and technology advancement

The Government shall promote indigenous digital innovation and support technology-driven entrepreneurship by—

(a) creating and implementing budgetary provisions for targeted grants, co-funded research partnerships, innovation competitions, and the commercialisation of locally developed digital technologies;
(b) providing fiscal and non-fiscal incentives, including tax reliefs, access to infrastructure, and capacity-building programs to qualified innovation-driven enterprises, research institutions, and technology hubs operating in emerging technology sectors;
(c) supporting the development, validation, and scale-up of indigenous solutions in fields including artificial intelligence, blockchain, quantum computing, financial technologies, digital identity systems, robotics, digital services, virtual or augmented reality, and extended reality; and
(d) facilitating the participation of Nigerian innovators in regulatory sandboxes, pilot programs, and government-supported test environments for the deployment and refinement of new digital solutions.

81. Process for subsidiary legislation

(1) The Regulatory Agency may, prior to making any regulation, guidelines or other subsidiary legislation under this Act, publish on its website, the draft regulation and a notice inviting written comments to be submitted on the proposed regulation within a stipulated time.

(2) Any regulation, guideline, or other subsidiary legislation made pursuant to this Act shall be published in the Federal Government Gazette.

82. Directives by the Minister, etc.

The Minister may give the Regulatory Agency such directives of a general nature relating to matters of policy with regard to the objectives of this Act as it may consider necessary, and it shall be the duty of the Regulatory Agency to comply with the directives or cause them to be complied with.

83. Interpretation.

In this Act, unless the context otherwise requires–

"addressee", in relation to an electronic communication, means a person who is intended by the originator to receive the electronic communication, but does not include a person acting as an intermediary with respect to that electronic communication;

"**artificial intelligence agents**" means any person, including public institutions, whether established in Nigeria or outside Nigeria, that develops, deploys, places on the market, operates, or otherwise makes available artificial intelligence systems that are used, intended to be used, or relied upon in Nigeria;

"**artificial intelligence system**" or "**AI system**" means a computational system, with varying degrees of autonomy, designed to achieve human-defined objectives by processing data and information to perceive and interpret its environment, interact with it, and generate outputs such as predictions, recommendations, classifications, or decisions that may affect physical or virtual environments; and such system may employ, without limitation,

(a) machine learning systems, including supervised, unsupervised, and reinforcement learning,
(b) systems based on knowledge representation and logic,
(c) statistical approaches, Bayesian inference, and optimisation methods, or
(d) generative AI, including deep and large language models capable of producing text, images, or other content based on training data;

"**asymmetric cryptosystem**" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

"authentication data" includes username, password and license key;

"automated system" means a computer programme or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by an individual, each time an action is initiated, or a response is generated by the program or electronic or other means;

"**Bayesian inference"** means a statistical method that updates the probability of a hypothesis or outcome by combining prior knowledge with new evidence or data, enabling artificial intelligence systems to make decisions or predictions under uncertainty;

"**Board of the Regulatory Agency**" has the meaning ascribed to it under the National Information Technology Development Agency Act, 2007.

"**certificate**" means a data message or other record confirming the link between a signatory and the signature creation data;

"**certified trust service**" means an electronic service normally provided for remuneration which consists of—

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, and certificates related to those services,
(b) the creation, verification, and validation of certificates for website authentication,
(c) the preservation of electronic signatures, seals, or certificates related to those services; and
(d) such other services as may be prescribed by the Regulatory Agency.

"**Commission**" has the meaning ascribed to it under the Federal Competition and Consumer Protection Act;

"consumer" means any person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier;

“**Coordinated Universal Time**” means the time scale maintained by the Bureau International des Poids et Mesures - International Bureau for Weights and Measures (BIPM), with assistance from the International Earth Rotation Service (IERS), which forms the basis of a coordinated dissemination of standard frequencies and time signals

"data" means any information presented in an electronic form;

"digital government services" means all services which are delivered by public institutions by electronic means;

“**digital literacy**” means the ability to use information and communication technology to find, evaluate, create, and communicate information, requiring both cognitive and technical digital skills at a basic level;

“digital signature” in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a hash function to authenticate electronic records, ensuring transformation into a secure electronic format and which complies with the requirements under section 16 of this Act.

"**digital technology services**” means services that involve the use, development, deployment, or management of digital technologies to enable, support, or enhance business operations, service delivery, or digital transformation.

“**e-Government platforms**” means digital systems, applications, or portals used by public institutions to deliver services, information, or administrative functions electronically to the public or across government agencies.

"e-Government initiative" means any intervention taken by a public institution for the purpose of implementing e-government;

“**electronic**” includes electrical, digital, magnetic, wireless, optical, electromagnetic, biometric, photonic, and similar capabilities;

"electronic communication" means any transfer of sign, signal, information or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, photo-optical or in any other similar form that is processed, recorded, displayed, created, stored, generated, received or transmitted in an electronic form;

“electronic form” with reference to information, means any information generated, sent, received or stored in media, magnetic form, optical form,

computer memory, micro portal, computer-generated microfiche or similar device;

“electronic gazette” means the electronic equivalent of the official Gazette of the Federal Republic of Nigeria to be created in accordance with this Act.

“electronic Government”, "e-Government" or “**digital government**” means the use of information and communication technologies (ICT) by the Government to deliver public services;

“electronic record” means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

“**electronic seal**” means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity.

“electronic signature” means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign;

"electronic transaction" includes transmission of data, information, documents or providing services electronically.

“electronic transferable record” means an electronic record that complies with the requirements of section 27;

“**emerging technologies**” means technologies characterised by rapid development, evolution, novelty, and uncertainty in trajectory and impact, and include blockchain and distributed ledger technologies, quantum computing, computer numerical control technologies such as 3D printing, and advanced robotics and autonomous systems;

“**emerging technologies agent**” means any person, including public institutions, whether established within or outside Nigeria, that develops, deploys, places on the market, operates, or otherwise makes available emerging technologies that are used, intended to be used, or relied upon within Nigeria;

"**Federal Government Printer**" means the Federal Government Press, responsible for the printing and publication of official government documents, including legislation, regulations, public notices, and other materials mandated for dissemination by the Federal Government of Nigeria;

“**hash function**” means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that —
(a) a record yields the same hash result every time the algorithm is executed using the same record as input;
(b) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm;
and
(c) it is computationally infeasible that two records can be found that produce the same hash result using the algorithm;
"ICT unit" includes a directorate, department, or unit responsible for ICT matters in a public institution;
“**individual**” means a natural person;
“**information**” includes data, text, documents, images, sounds, codes, computer programmes, software, and databases;
“information system” or “information technology system” includes a system for generating, sending, receiving, storing, or otherwise processing an electronic record;
“intermediary” with respect to an electronic communication, means a person who, on behalf of another person, sends, receives, transmits, or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes the provision of mere conduit, caching and hosting services;
"interoperability" means the ability of different information technology systems and software applications to communicate, exchange data, and use of information that has been exchanged;
“**key pair**”, in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;
“**Minister**” means the minister with the responsibility for communications and digital economy.
“originator” in relation to electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication;
"public institution" means ministries, departments, agencies, executive agencies, parastatals, organisations, public corporations, or any other Government autonomous or semi-autonomous institutions;

“**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;
“record” includes information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based, or other medium and is retrievable in visible form;
“**quantum computer”** means a computer that uses the collective properties of quantum states to perform calculations;
“Regulatory Agency” means the National Information Technology Development Agency;
“**security procedure**” means a procedure established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that a digital signature, communication, or performance is that of a particular person or for detecting changes or errors in the content of an electronic communication;
"service provider" means an organisation, business, or individual that offers electronic service to a public institution;
“signatory” means an individual who creates an electronic signature;
“**signed” or** “**signature**” and its grammatical variations mean a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record;
“**signature creation data**” means unique data, including codes or private cryptographic keys or a uniquely configured physical device, which is used by the signatory in creating an electronic signature;
“supplier” means a person who uses electronic means in providing goods or services or both;
“trust service provider” means a person who provides certified trust services;
“**time stamp**” means a data unit created using a system of technical and organisational means that certifies the existence of electronic data at a given time;
“**transaction**” means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including the sale, lease, exchange, licensing or other disposition of personal property, including goods and intangible interests in real property, services, or any combination of any of these acts;
“**transferable document or instrument**” means a document or an instrument issued on paper that entitles the holder to claim the performance

of the obligation indicated in the document or instrument and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument, and includes —

(a) a bill of exchange;
(b) a promissory note; and
(c) a bill of lading.

84. Short Title

This Act may be cited as the National Digital Economy and E-Governance Act, 2025.