Draft
ELECTRONIC COMMERCE DECREE-LAW

Democratic Republic of Timor-Leste

Electronic commerce (e-commerce) plays a critical role in economic growth and development. It lowers transaction costs for business, consumers and government, extends the geographic reach within which products and services may be bought and sold, and through online transactions, dramatically increases the range of products and services that are available. Electronic commerce also supports cross-border trade and facilitates efficiency initiatives such as the National Single Window. But e-commerce requires an effective, comprehensive legal environment in order to flourish in the evolving interconnected world.

Hence, the purpose of this Decree-Law is to provide Timor-Leste with a legal regime that will promote the development of electronic commercial transactions within the broader scope of the information society, offering significant investment and employment opportunities while stimulating economic growth and innovation.

To that effect, the opportunity has been taken in preparing this Decree-Law to address certain underlying issues beyond the scope of commercial transactions that are deemed necessary to ensure the effectiveness of this legislative initiative; for example, provisions governing the validity of contracts executed by electronic means, the use of electronic records and the legal status of electronic signatures.

Thus, this Decree-Law will, among other things, establish the legal equivalence of online and paper-based transactions (including both governmental and private sector transactions). Moreover, this Decree-Law establishes requirements for the execution and acceptance of electronic contracts and records, permits the use of electronic signatures, establishes requirements governing online transactions, including the specification of information to be provided to consumers by electronic commerce providers, and adopts the principle of technological neutrality with respect to electronic signatures and records. In addition, it sets standards for the use of unsolicited commercial electronic mail (commonly known as “spam”), defines and prohibits the use of fraudulent electronic mail, and provides a mechanism for and jurisdiction over the resolution of disputes concerning online commercial transactions.

This Decree-Law also establishes the principle of nondiscrimination as between domestic and foreign e-signatures and e-records, recognizes the legitimacy of foreign e-signatures and e-records in Timor-Leste and, in so doing, is intended to facilitate international trade.

As recognized in the National Policy for Information and Communications Technologies (ICT), this Decree-Law will also facilitate the interaction and involvement of citizens and businesses with the government of Timor-Leste in both domestic and international matters. The adoption of this Decree-Law will also encourage the development of cross-border paperless trade, thereby supporting increased integration of

Timor-Leste into the broader regional and global economy. To that end, Timor-Leste will cooperate with other countries in facilitating and encouraging the use of e-commerce.

This Decree-Law is intended to reflect international best practice. That includes, but is not limited to, **t**he UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures and the UNCITRAL Model Law on Electronic Transferable Records.

This Decree-Law is intended to be technology-neutral. Moreover, recognizing that technology will continue to develop, this Decree-Law is intended to be applied in a flexible fashion that will permit the application of such new technologies in an appropriate manner, consistent with the purposes and intent of this Decree-Law.

Thus, the Government decrees, pursuant to subparagraphs e) and o) of paragraph (1) of Article 115, and of subparagraph d) of Article 116 of the Constitution of the Democratic Republic of Timor-Leste to be effective as law, the following:

CHAPTER I
GENERAL PROVISIONS

ARTICLE 1
Purpose

This Decree-Law establishes the general legal regime applicable to electronic records, signatures and transactions and with particular reference to their use in the field of electronic commerce.

ARTICLE 2
Application of the Law

1. This Decree-Law shall govern the conduct of electronic commerce ("e-commerce") in Timor-Leste and shall apply to any natural person or legal entity that sells or offers to sell any services or goods via e-commerce to any natural person or legal entity domiciled, headquartered or established in Timor-Leste.
2. By virtue of any such activity purposely directed to the marketing and sale of services and goods in Timor-Leste, any such natural person or legal entity shall be deemed to be doing business in Timor-Leste and to be subject to its jurisdiction whether or not such natural person or legal entity has a physical or legal presence in Timor-Leste.
3. The provisions of this Decree-Law shall also apply to the execution and acceptance of electronic records, the use and legal status of electronic signatures, and the conclusion of contracts by electronic means, whether or not they refer to e-commerce, whenever Timor-Leste law is chosen by the parties or is otherwise deemed to be applicable.
4. The provisions of this Decree-Law shall be without prejudice to the application of compatible legislation in force, such as related provisions in the fields of telecommunications services, trade and customs, data protection and consumer protection that result from6other relevant national legislation.

ARTICLE 3

Exclusions from Scope

This Decree-Law shall not apply to the following matters, except where use of electronic records and communications satisfies particular legal requirements for their authenticity:

a) Wills, codicils, testamentary trusts or other matters of succession law;
b) Marriage, adoption, divorce or other matters of family law;
c) The transfer of real property and any real estate matters requiring notarial intervention;
d) Any other documents whose validity depends on notarial intervention;
e) Official court documents, including court order or notices;
f) Notification of cancellation or termination of utility services;
g) Default, acceleration, repossession, foreclosure or eviction, or the right to cure under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
h) Cancellation or termination of health insurance benefits or life insurance benefits;
i) Securities, such as shares and bonds, and other investment instruments; and
j) Recall of a product or notice of material failure of a product that risks endangering health or safety.

ARTICLE 4

Definitions

The following definitions shall apply to this Decree-Law:

a) The term “addressee” of an electronic communication means a party who is intended by the originator to receive the electronic communication but does not include a party acting as an intermediary with respect to that electronic communication.
b) The term “automated electronic system” means a computer program 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 a natural person each time an action is initiated or a response is generated by the system.
c) The term “bill of exchange” means a signed and dated unconditional written order whereby the drawer directs the drawee to pay a definite sum of money to the payee or to his order on demand or at a definite time.
d) The term “bill of lading” means the commercial document, with a unique number which is required for the movement of all goods across customs borders, serving as proof of the terms and conditions of transport agreed between the two parties (importer and supplier).
e) The term “Certificate” means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of a person who holds a particular key pair.
f) The term “Certification Service Provider” means a legal person that issues a Certificate.
g) The term “commercial electronic mail message” means any electronic mail message, the primary purpose of which is the advertising or promotion of a commercial product or service; provided,

DRAFT

however, that it does not mean an electronic mail message concerning an order of a product or service from the sender generated by the recipient of the electronic message.

h) The term “communications” means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract.

i) The term “consumer” means any natural or legal person to which goods are supplied or services are provided for a non-business use by a person carrying on an economic activity, in the nature of a business, with a view to the obtaining of benefits.

j) The term “data message” means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, electronic messaging, telegram, telex or telecopy; where the data message is sent using an electronic network, the term “electronic data message” may also be used.

k) The term “electronic commerce” or “e-commerce” refers to activities involving the purchase, sale, rental, or exchange of goods or services, by consumers, business and/or governments, entirely within Timor-Leste or in a cross-border transaction, where such activities are transacted or facilitated by means of electronic communication, including but not limited to, financial transactions conducted over electronic data interchanges. The term “electronic commerce” also includes “mobile commerce” or “m-commerce” as defined herein.

l) The term “electronic communication” means any communication that the parties to a e-commercial transaction make by means of data messages or electronic networks.

m) The term “e-commerce merchant” means any natural or legal person engaged in commerce in Timor-Leste that offers services and/or goods for sale, lease or exchange to customers, including public entities, in Timor-Leste or elsewhere by means of an electronic transaction. This term also means any natural or legal person outside of Timor-Leste that offers services and or goods for sale, lease or exchange to customers within Timor-Leste, but does not include any intermediary as defined herein.

n) The term “electronic data interchange” means the transfer of data between two computer systems in a standard electronic format without human intervention.

o) The term “electronic record” means a record that is made, communicated, received, stored or processed in an electronic system or in any system or device used for transmission from one electronic system to another.

p) The term “electronic signature” means an electronic sound, symbol or process used to identify a person and to indicate that person’s approval of and intent to be bound by a contract or information.

q) The term “electronic transferable record” means an electronic record that complies with all the requirements of Chapter IV of this Decree-Law.

r) The term “government entity” means any ministry, department, public institute or other entity of the Direct, Indirect or Autonomous State Administration of Timor-Leste, including but not limited to local government entities, that performs the functions set forth in Article 17, paragraph (1) below.

s) The term “information” means information (whether in its original form or otherwise) that is in the form of a document, a signature, a seal, data, text, images, sound or speech.

t) The term “information system” means a system for producing, sending, receiving, storing, displaying or otherwise processing electronic communications or information.

u) The term “intermediary” means a person or legal entity who, on behalf of another person or legal entity, sends, receives or stores, either on a temporary or permanent basis, the electronic communication or provides other services relating to the electronic communication, but does not originate the content that is sent, received or stored.

v) The term “key pair” refers to the public and private digital keys that are used to verify the identity of a signatory to a digital or electronic transaction.

w) The term “Minister” means the cabinet member responsible for the area of Commerce.

x) The term “Ministry” means the Ministry responsible for the area of Commerce.

y) The term “mobile commerce” or “m-commerce” means the use of wireless handheld devices, including but not limited to mobile phones, to conduct electronic commerce and includes the use of such devices to conduct online financial transactions.

z) The term “place of business” means any place where a party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services at a specific location.

aa) The term “promissory note” means a signed and dated written unconditional promise whereby the maker undertakes to pay a definite sum of money to the payee or his order and is payable on demand or at a definite time.

bb) The term “originator” of an electronic communication means a person or entity, 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.

cc) The term “secure electronic signature” means an electronic signature that has been confirmed by technological means, including, but not limited to, a Public Key Infrastructure (PKI) Certificate, to be unique to the person using it and which satisfies the other requirements of this Decree-Law concerning such signatures.

dd) The term “Signatory” means a person or legal entity that holds signature certification data and that acts either on its own behalf or on behalf of the person it represents.

ee) The term “Spam” means unsolicited commercial electronic mail messages.

ff) The term “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 but is not limited to:

i) a bill of exchange;
ii) a bill of lading; and
iii) a promissory note.

ARTICLE 5

Effectiveness and Non-Discrimination

DRAFT

1. Whether, or to what extent, an electronic record, certificate or an electronic signature, or an electronic transferable record is legally effective shall be determined based on its reliability pursuant to Article 6 of this Degree-Law.
2. In making that determination, no regard shall be given to the following, whether or not such geographic location is inside or outside Timor-Leste:
    a) To the geographic location where the certificate is issued or the electronic signature, electronic record or electronic transferable record is created or used; or
    b) To the geographic location of the place of business of the issuer, signatory, creator or user.
3. A Certificate issued or used outside of Timor-Leste shall have the same legal effect in Timor-Leste as a Certificate issued in Timor-Leste if it offers a substantially equivalent level of reliability.
4. An electronic signature created or used outside of Timor-Leste shall have the same legal effect in Timor-Leste as an electronic signature created or used in Timor-Leste if it offers a substantially equivalent level of reliability.
5. An electronic record issued or used outside of Timor-Leste shall have the same effect in Timor-Leste as an electronic record created or used in Timor-Leste shall have the same effect in Timor-Leste as an electronic record created or used in Timor-Leste if it offers a substantially equivalent level of reliability.
6. An electronic transferable record issued or used outside of Timor-Leste shall have the same effect in Timor-Leste as an electronic transferable record created or used in Timor-Leste if it offers a substantially equivalent level of reliability.
7. In determining whether an electronic record, certificate or an electronic signature, or an electronic transferable record offers a substantially equivalent level of reliability, due regard shall be given with respect to recognized international standards.
8. Notwithstanding the provisions of this Article, where parties agree between themselves to the use of certain types of electronic signatures or certificates, electronic records or electronic transferable records, that agreement shall be recognized as sufficient for the purposes of cross-border recognition unless that agreement would not be valid or effective under applicable law.

ARTICLE 6
Reliability

When this Decree-Law imposes a reliability requirement, the reliability of such method for an electronic record, certificate or electronic signature, or an electronic transferable record shall be:

a) As reliable as appropriate for the fulfilment of the purpose or function for which the method is being used, in the light of all the relevant circumstances, which may include but are not limited to the following:
    i) Any operational rules relevant to the assessment of reliability;
    ii) The assurance of data integrity;
    iii) The ability to prevent unauthorized 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 a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;
vii) Any relevant agreement;
viii) Any applicable industry standard; or
ix) Compliance with recognized international standards.

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

ARTICLE 7
Place of business

1. For the purposes of this Decree-Law, a location is not a place of business merely because it is:
   a) Where equipment and technology supporting an information system used by a party in connection with electronic transferable records are located; or
   b) Where the information system may be accessed by other parties.
2. The sole fact that a party makes use of an electronic address or other element of an information system connected to a specific country does not create a presumption that its place of business is located in that country.

ARTICLE 8
Information requirements

Nothing in this Decree-Law affects the application of any rule of law that may require a person to disclose its identity, place of business or other information, or relieves a person from the legal consequences of making inaccurate, incomplete or false statements in that regard.

CHAPTER II
ELECTRONIC RECORDS AND SIGNATURES

ARTICLE 9
No Obligation to Use Electronic Records

1. Nothing herein obligates any party to use, provide or accept information in electronic form without that person's consent.
2. With respect to transactions between parties, the provisions of this Decree-Law shall apply only to transactions where each party has agreed that the transaction will be conducted by electronic means.
3. Such agreement may be explicitly stated by the parties; it may also be determined from the context and circumstances, including the conduct of the parties to the transaction.
4. However, the parties to a written form contract shall not be bound to use electronic means by virtue of a provision in such form contract unless that requirement is conspicuously set forth in larger print than contained in the rest of such form contract and is separately agreed to by the parties.

DRAFT

5. Agreement to conduct a transaction by electronic means does not obligate either party to conduct any other transaction by electronic means and either party may refuse to conduct any other transaction by electronic means.
6. The parties to a transaction may, by agreement, impose additional requirements as to the form or authentication of the contract or transaction beyond those specified by this Decree-Law.

ARTICLE 10
Validity of Electronic Records

1. Notwithstanding the provisions of any other law, rule or regulation, a document, record or signature may not be denied legal effect, including being used as evidence in a judicial proceeding, or enforceability solely because it is:
    a) In electronic form or is in an electronic communication; or
    b) Referred to in an electronic communication that is intended to give rise to that legal effect.
2. Where there is a legal requirement that information is to be in writing or provides for certain consequences if such information is not in writing, an electronic record satisfies that legal requirement if the information contained therein is accessible so as to be usable for subsequent reference.

ARTICLE 11
Retention of Electronic Records

1. Where a law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are satisfied:
    a) The information contained therein remains accessible so as to be usable for subsequent reference;
    b) The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and
    c) Such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained.
2. An obligation to retain documents, records or information in accordance with paragraph (1) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.
3. Nothing in this Article shall:
    a) Supersede any law which expressly provides for the retention of documents, records or information in the form of electronic records; or
    b) Preclude any department or ministry or organ of State from specifying additional requirements for the retention of electronic records that are subject to the jurisdiction of such department or ministry or organ of State.

ARTICLE 12
Original Documents

DRAFT

1. Where there is a legal requirement that a document, record or information be presented or retained in its original form, or provides for certain consequences if it is not, that requirement is met by providing or retaining the document, record or information in the form of an electronic record if:
    a) There exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form whether as a document in writing or as an electronic record; and
    b) Where it is required that the document, record or information be presented, that such document, record or information is capable of being displayed to the person to whom it is to be presented.
2. For the purposes of subparagraph a) of paragraph (1):
    a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the introduction of any immaterial changes that arise in the normal course of communications, storage and display; and
    b) The standard of reliability required shall be as defined in Article 6 of this Decree-Law.

ARTICLE 13

Electronic Signatures

1. Where a law requires a signature, or provides for certain consequences if a document or a record is not signed, or if the parties to a transaction agree that an electronic signature is required, the requirement is satisfied in relation to an electronic record by an electronic signature if:
    a) A method is used to identify the person and to indicate that person's intention with respect to the information contained in the electronic record and
    b) The method used is determined to be reliable in accordance with the standards specified in Article 6 of this Decree-Law
2. Where a law requires, or the parties to a transaction specify, that a secure electronic signature be utilized, such a requirement is satisfied if, it can be verified that an electronic signature at the time it was executed was:
    a) Unique to the person using it;
    b) Capable of identifying such person;
    c) Created in a manner or using a means under the sole control of the person using it; and
    d) Linked to the electronic record to which it relates in a manner such that if the record was altered, the electronic signature would be rendered invalid.

For purposes of this verification, any reasonable method may be used, including but not limited to a Certificate issued under the procedures specified in this Decree-Law or a commercially reasonable security procedure agreed to by the parties involved.

3. Except to the extent that parties to an agreement may otherwise agree, nothing in this Decree-Law shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements of either paragraph (1) or paragraph (2).

ARTICLE 14

Certification Service Provider

1. In order to be authorized to operate as a Certificate Service Provider, a legal person must be duly authorized by the Minister.
2. A legal person may apply for recognition as a Certification Service Provider, through the submission to the Ministry of an application fulfilling the requisites and criteria that may be determined by the Minister through Ministerial Diploma. The Minister may grant such recognition to a foreign entity so long as it satisfies the requirements of this Article. Such recognition shall not be a requirement for recognition of a Certificate issued outside of Timor-Leste so long at it satisfies the requirements of Article 5 of this Decree-Law.
3. The requisites and criteria determined by the Minister shall take into account the following factors:

    a) Independence (i.e., absence of financial or other interest in underlying transactions);
    b) Financial resources and financial ability to bear the risk of being held liable for loss;
    c) Expertise in public-key technology and familiarity with proper security procedures;
    d) Longevity (certification authorities may be required to produce evidence of certification or decryption keys many years after the underlying transaction has been completed, in the context of a lawsuit or property claim);
    e) Approval of hardware and software;
    f) Maintenance of an audit trail and audit by an independent entity;
    g) Existence of a contingency plan (e.g., “disaster recovery” software or key escrow);
    h) Personnel selection and management;
    i) Protection arrangements for the certification service provider’s own private key;
    j) Internal security;
    k) Arrangements for termination of operations, including notice to users;
    l) Warranties and representations (given or excluded);
    m) Limitation of liability;
    n) Insurance;
    o) Interoperability with other certification authorities; and
    p) Revocation procedures (in cases where cryptographic keys might be lost or compromised)

4. The duties of such a Certification Service Provider shall be as follows:
    a) Act in accordance with representations made by it with respect to its policies and practices;
    b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;
    c) Provide reasonably accessible means that enable a relying party to ascertain from the Certificate:
        i) the identity of the Certification Service Provider;
        ii) that the signatory identified in the certificate had control of the signature creation data at the time when the certificate was issued;
        iii) that signature creation data were valid at or before the time when the certificate was issued.
    d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:

i) the method used to identify the signatory;
ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
iii) that the signature creation data are valid and have not been compromised;
iv) any limitation on the scope or extent of liability stipulated by the Certification Service Provider;
v) whether means exist for the signatory to give notice pursuant to Article 15, paragraph (1), b) of this Decree-Law;
vi) whether a timely revocation service is offered.

e) Where services under Article 15, paragraph (1), b) are offered, provide a means for a signatory to give notice pursuant to Article 15, paragraph (1), b) of this Decree-Law and where services under subparagraph (d) (vi) of this Article are offered, ensure the availability of a timely revocation service.
f) Utilize trustworthy systems, procedures and human resources in performing its services.

5. A Certification Service Provider shall be legally liable for its failure to satisfy the requirements of this Article

ARTICLE 15
Signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
   a) Exercise reasonable care to avoid unauthorized use of its signature creation data;
   b) Without undue delay, utilize means made available by the Certification Service Provider pursuant to Article 14 of this Decree-Law, or otherwise use reasonable efforts, to notify any person who may reasonably be expected by the signatory to rely on to provide services in support of the electronic signature if:
      i) the signatory knows that the signature creation data have been compromised; or
      ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised.
   c) Where a Certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certification.
2. A signatory shall be legally responsible for its failure to satisfy the requirements of this Article under the general terms of civil and contractual liability.

ARTICLE 16
Relying Party

A relying party shall be legally responsible for its failure:

a) To take reasonable steps to verify the reliability of an electronic signature; or

b) To take reasonable steps, where an electronic signature is supported by a Certificate:
   i) To verify the validity, suspension or revocation of the Certificate; and
   ii) To observe any limitation with respect to the Certificate.

ARTICLE 17
Use of Electronic Records and Signatures by Government Agencies

1. Any government entity that performs any of the following functions may, notwithstanding any law to the contrary, perform that function or functions by means of electronic records or in electronic form:
   a) Accepts the filing or submission of documents or information;
   b) Requires the creation or retention of documents or other information;
   c) Requires documents, records or information to be provided or retained in their original form.
   d) Issues any permit, license or approval; or
   e) Issues a prescribed form for an application or notification to or other transaction with the government entity; or
   f) Requires payment of any fee, charges, tax or other amount by any method and manner of payment.
2. In any case where a government entity decides to perform any of the functions in paragraph (1) by means of electronic records or in electronic form, such government entity shall provide the following information, through one or more means that ensure it is easily accessible by the interested public, including but not limited to, publication in the official gazette and the official website of the government entity:
   a) The manner and format in which electronic records shall be submitted, created, retained, issued or provided;
   b) In the event that such electronic records must be signed, the type of electronic signature required (such as a secure electronic signature or the particular type of secure electronic signature);
   c) The manner and format in which such signature shall be affixed to the electronic record and the identity of or criteria that shall be met by any specified security procedure provider used by the person filing the document;
   d) Such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and
   e) Any other required attributes for electronic records or payments.
3. Where any natural or legal person is required by law to perform, file, create, retain, submit or provide any of the documents, records or applications set forth in paragraph (1) and performs such functions through an electronic record or document or with an electronic signature, such a requirement is satisfied so long as the electronic record, document or signature is submitted in the manner and fashion, and in compliance with, the requirements of paragraph (2).
4. Nothing in this Article shall, by itself, require any government entity to accept or issue any document or information in the form of electronic records or to accept any payment in electronic form.

DRAFT

ARTICLE 18
Private Agreements

Notwithstanding the provisions of Article 5 of this Decree-Law, where parties agree between themselves to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition unless that agreement would not be valid or effective under applicable law.

CHAPTER III

ELECTRONIC TRANSACTIONS

ARTICLE 19
Formation of Electronic Contracts

1. A contract shall not be denied legal effect, validity or enforceability solely because an electronic communication, an electronic record or an electronic signature was used in its formation.
2. Unless otherwise agreed by the parties or specifically provided by another law, the communications of proposals, acceptance of proposals, and revocation of proposals and acceptances or any related communications may be expressed through electronic means.
3. Except to the extent that the parties may otherwise agree, electronic contracts may be formed through an offer and acceptance of an offer expressed by electronic means as follows:

a) **Time of dispatch**

An electronic communication shall be deemed to be sent at the time the electronic communication first leaves an information system under the control of the originator or the party who sent it on behalf of the originator.

b) **Time of receipt**

An electronic communication shall be deemed to have been received at the time that an electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee or in any other case, at the time that the addressee becomes aware that the electronic communication has been sent.

c) **Place of dispatch**

An electronic communication is deemed to be sent from:

i) the originator's place of business; or
ii) if the originator has more than one place of business, the place of business that has the closest relationship with the underlying transaction; or
iii) if there is no place of business to which subparagraph (i) applies, the originator's principal place of business; or
iv) in the case of an originator who does not have a place of business, the originator's ordinary place of residence.

d) **Place of receipt**

An electronic communication is deemed to be received at:

i) the addressee's place of business; or

ii) if the addressee has more than one place of business, the place of business that has the closest relationship with the underlying transaction; or

iii) the addressee's principal place of business if there is more than one place of business and there is no place of business to which subparagraph (ii) applies; or

iv) in the case of an addressee who does not have a place of business, the addressee's ordinary place of residence.

e) **Time of communication of acceptance of offer**

For the purpose of the formation of a contract, an acceptance by electronic communication of an offer is taken to be communicated to the offeror at the time determined by paragraph (3), subparagraph b) (Time of Receipt) to be the time of receipt for that electronic communication.

4. A contract may be formed through the interaction of an automated electronic system and an individual, acting on the individual's own behalf or for another person, including an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.
5. In the event that a contract is formed through the interaction of an automated electronic system and a natural person, it shall not be denied validity solely on the ground that no natural person reviewed or intervened in the actions carried out by the automated system or the resulting contract.
6. In the event that a natural person makes an input error in an electronic communication exchanged with an automated electronic system of another party and that system does not provide the natural person with an opportunity to correct the error, that person, or the person on whose behalf that person was acting, has the right to withdraw the electronic communication in which the error was made; provided, however, that this paragraph shall not apply unless:
   a) The natural person, or the person on whose behalf that person was acting, notifies the other party of the error as soon as possible after having made or learned of the error and indicates that he or she made an error in the electronic communication;
   b) Takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record and
   c) Has not used or received any material benefit or value from the goods or services, if any, received from the other party.
7. A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

DRAFT

ARTICLE 20
Obligations of E-Commerce Merchants

1. Each merchant engaged in e-commerce or that utilizes e-commercial systems or services (hereinafter designated "e-commerce merchant") shall provide the following information related to use of e-commerce services and such information shall be prominently displayed on the provider's e-commerce electronic marketing and sales site:
    a) The name of the e-commerce merchant;
    b) The Tax Identification Number or, for merchants who have their place of business outside of Timor-Leste, the equivalent taxpayer identification or registration number issued by the competent authorities of that place of business;
    c) The geographic address where the e-commerce merchant is located;
    d) The contact information of the e-commerce merchant, including at least one telephone number and that merchant's electronic mail address;
    e) The price for any services or products offered on its electronic marketing and sales site, including the currency in which the price is charged;
    f) The alternatives, if any, for delivery of the product or service, the delivery charge for each such alternative, and the estimated delivery charge for the product or service ordered;
    g) A method for reviewing and cancelling an order before it is finally placed by the consumer.
    h) The terms and conditions that apply to the use of the e-commerce electronic marketing and sale site; such terms and conditions shall include, but are not limited to:
        i) information concerning the submission of consumer complaints regarding the e-commerce merchant and/or products or services offered by such merchant, including the name, email address and telephone number of the individual or office to which such complaints should be submitted;
        ii) the method and geographic location for resolving any disputes concerning any online purchase of services or products that cannot be resolved through the complaint process set forth in subparagraph (i) herein; provided that if the location for dispute resolution is not in Timor-Leste, the terms and conditions shall specify an online dispute resolution mechanism, providing for mediation by a neutral third party to resolve the consumer complaint. This shall not preclude machine-based dispute resolution, such as provided by means of Artificial Intelligence. In the event that mediation does not resolve the complaint, the terms and conditions may specify that arbitration shall be used to resolve the dispute. Such arbitration shall take place online and shall otherwise conform to the standards set forth in the Timor-Leste Voluntary Arbitration Law;
        iii) a statement that the e-commerce merchant complies with the applicable data privacy and protection law and provides an online link to that law, if it exists; and
        iv) a statement that the e-commerce merchant complies with the provision of Article 21 of this Decree-Law concerning Spam.
2. Secure technology and protocols must be used to safeguard the transmission and receipt of online payment and other private or sensitive information.

3. For any product or service ordered from the e-commerce merchant, the following information shall be provided to the purchaser prior to the finalization of the purchase:
   a) The total price of the product or service, including any currency conversion charge, tax or delivery charge for the selected method of delivery, each of which shall be separately identified and listed;
   b) The methods of payment accepted by the e-commerce merchant;
   c) The alternatives for return, repair or replacement of a purchased product, and the time periods applicable to each, in the event that the product delivered to the consumer is defective or is inconsistent with the description of the product as presented on the e-commerce merchant's electronic marketing and sales site; and
   d) The period of time and method by which a product delivered to the consumer may be returned to the seller, said period of time shall be not less than seven (7) business days, and the allocation of costs, if any, between the seller and customer for any such returned product; provided that, if the reason for the return is that the product is defective or does not comply with the description of the product provided by the e-commerce merchant prior to its sale to the purchaser, the seller shall bear the entire cost of returning the product.
4. An e-commerce merchant shall not produce or post reviews of products or services that it knows, or should reasonably know, are false or do not reflect that actual use of the product or service by consumers, with the provisions of Articles 6 and 7 of the Consumer Protection Law of Timor-Leste being hereby incorporated by reference.

ARTICLE 21
Spam

1. It is unlawful for any sender of a Commercial Electronic Mail Message to send such a message without including in that message a return electronic email address that is functional for at least 30 days after the transmission of the original message or provides another clearly displayed and readily accessible mechanism by which the recipient of such message may submit, by electronic mail or other electronic -based communication, a request not to receive future such messages from the sender at the specified electronic mail address.
2. It is unlawful to send a Commercial Electronic Mail Message when the recipient has made a request not to receive such messages from a specific sender more than ten (10) business days prior to the transmission of such unsolicited electronic message.

CHAPTER IV

ELECTRONIC TRANSFERABLE RECORDS

ARTICLE 22
Scope of application

DRAFT

1. This Chapter applies to electronic transferable recordsI.
2. Other than as provided for in this Decree-Law, nothing in this Decree-Law affects the application to an electronic transferable record of any rule of law governing a transferable document or instrument, including any rule of law applicable to consumer protection.

ARTICLE 23
Transferable documents or instruments

1. Where the law requires a transferable document or instrument, that requirement is 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) A reliable method is used:
        i) to identify that electronic record as the electronic transferable record;
        ii) to render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and
        iii) To retain the integrity of that electronic record.
2. The criterion for assessing integrity shall be whether information contained in the electronic transferable record, including any authorized change that arises from its creation until it ceases to have any effect or validity, has remained complete and unaltered apart from any change which arises in the normal course of communication, storage and display.
3. Nothing in this Decree-Law precludes the inclusion of information in an electronic transferable record in addition to that contained in a transferable document or instrument.

ARTICLE 24
Control

1. Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:
    a) To establish exclusive control of that electronic transferable record by a person; and
    b) To identify that person as the person in control.
2. Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

ARTICLE 25
Indication of time and place in electronic transferable records

Where the law requires or permits the indication of time or place with respect to a transferable document or instrument, that requirement is met if a reliable method is used to indicate that time or place with respect to an electronic transferable record.

ARTICLE 26
Endorsement

Where the law requires or permits the endorsement in any form of a transferable document or instrument, that 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 Article 10, paragraph (2), and Article 13 of this Decree-Law.

ARTICLE 27
Amendment

Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such.

ARTICLE 28
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 a reliable method for the change of medium is used.
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 paragraphs 1 and 2, the transferable document or instrument shall be made inoperative and ceases to have any effect or validity.
4. A change of medium in accordance with paragraphs 1 and 2 shall not affect the rights and obligations of the parties.

ARTICLE 29
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 reliable method for the change of medium is used.
2. For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the transferable document or instrument.

3. Upon issuance of the transferable document or instrument in accordance with paragraphs 1 and 2, the electronic transferable record shall be made inoperative and ceases to have any effect or validity
4. A change of medium in accordance with paragraphs 1 and 2 shall not affect the rights and obligations of the parties.

ARTICLE 30

Private International Law

Nothing in this Decree-Law affects the application to electronic transferable records of rules of private international law governing a transferable document or instrument.

CHAPTER V
SUPERVISION AND SANCTIONS

ARTICLE 31

Powers and responsibility of the Ministry

It is incumbent upon the Ministry, where such duties are not incumbent upon other bodies:

a) To establish regulations on practices to be followed in to order to comply with the provisions of this Decree-Law;
b) To monitor compliance with the rules on electronic records and signatures and the rules on electronic commerce;
c) To supply information to Certification Service Providers, Signatories and the general public, where requested;
d) To order the opening of breach proceedings and to carry on the respective investigation, as well as to apply the sanctions provided for.

ARTICLE 32

Administrative Offences

1. The following infractions shall constitute administrative offences liable to a fine ranging from USD [***] to USD [***]:

a) Failure by Certification Service Providers to comply with the obligations provided for under Article 10 of this Decree-Law;
b) Failure by e-commerce merchants to comply with the obligations provided for under Article 16 of this Decree-Law;
c) Messaging of spam in violation of the legal requirements provided for in Article 18
d) Failure to provide information requested by the supervisory entity referred to in Article 32 of this Decree-Law.

2. The following infractions shall constitute administrative offences liable to a fine ranging from USD [***] to USD [***]:
3. Negligence shall be punishable within the limits of the fine applicable to offences provided for in paragraph 1.
4. Where the offence is committed by someone other than a natural person, the fine shall be increased by one-third in respect of both its maximum and minimum amount.
5. The amount of the fine to be imposed on the offender, under the terms of this Article, is set by taking into account the seriousness of the infraction which shall be determined by the following factors:

    a) The extent of the damage caused;
    b) The amount of economic harm resulting from the infraction;
    c) The frequency and duration of the conduct by which the offense was committed;
    d) Whether the harm caused was reasonably foreseeable;
    e) Whether the infringement was an offense for which the offender had previously been sanctioned;
    f) The financial situation of the person who committed the offence;
    g) Whether the conduct was intentionally harmful; and
    h) Whether any compensation has been paid to any injured party.

ARTICLE 33
Applicable rules

1. The regime established under this Chapter is without prejudice to the special administrative sanctions' regimes in force.

2. The general legal regime of administrative offences against the economy and food security, contained in Decree-Law No. 23/2009, of 5 August, as may be amended from time to time, shall apply subsidiarily.

CHAPTER VI
FINAL PROVISIONS

ARTICLE 34
Entry into Force

This Decree-Law shall come into force on the ninetieth day following its publication.

Approved by the Council of Ministers, on [date].

The Prime Minister,

_____
Taur Matan Ruak

The [***],

_____
[***]

DRAFT