WORKING DRAFT (20 MAY 2016)

INDEPENDENT STATE OF PAPUA NEW GUINEA

A BILL

for

AN ACT

Entitled

Electronic Transactions Act 2018

INDEPENDENT STATE OF PAPUA NEW GUINEA

A BILL

for

AN ACT

Entitled

Electronic Transactions Act 2018

PART I. – PRELIMINARY.

1. Interpretation.
   "addressee";
   "automated message system";
   "certificate";
   "commercial";
   "communication";
   "data message";
   "electronic data interchange (EDI)";
   "electronic record";
   "electronic transferable record";
   "electronic signature";
   "information system";
   "intermediary";
   "non-commercial";
   "originator";
   "party";
   "place of business";

40. Extent of liability of a service provider.
41. Lawful access.
42. Obligation of confidentiality.
43. Penalties.

INDEPENDENT STATE OF PAPUA NEW GUINEA

A BILL

for

AN ACT

Entitled

Electronic Transactions Act 2018

Being an Act to –

(*a*) establish a legal framework for the use of electronic transactions for commercial and non-commercial purposes; and

(*b*) enable the legal framework for the use of electronic transactions, which implies-

(i) facilitation of electronic communications by means of reliable electronic records; and

(ii) facilitation of electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce; and

(iii) facilitation of electronic filing of documents with public agencies, and to support the promotion of efficient delivery by public agencies of services by means of reliable electronic records; and

(iv) by application of principles relevant to electronic transactions minimization of the incidences of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions; and

(v) help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(vi) promotion of public confidence in the integrity and reliability of electronic records and electronic commerce, and foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Made by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting with, and in accordance with the advice of the Minister.

PART I. – PRELIMINARY.

1. INTERPRETATION.

(1) Unless the contrary intention appears-

"addressee" of an electronic communication means a person 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;

"automated message 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;

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

"commercial" means relating to or connected with trade and traffic or commerce in general;

"communication" 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;

"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, telegram, telex or telecopy;

"electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

"electronic record" means information generated, communicated, received or stored by electronic means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not;

"electronic transferable record" is an electronic record that complies with the requirements of Section 32;

"electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message;

"information system" means a system for generating, sending, receiving, storing or otherwise processing data messages;

"intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

"non-commercial" refers to any activity or entity that does not involve commerce or trade;

"originator" of an electronic communication means a person by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that electronic communication;

"party" means any person (legal or natural) involved in a transaction or proceeding;

"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 out of a specific location;

"relying party" means a person that may act on the basis of an electronic signature;

"service provider" means a person that provides services related to electronic signatures, including by issuing and managing certificates;
"signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
"transaction" means a communication involving two or more persons that affects all those involved or the act or process of transacting;
"transferable document or instrument" means a document or 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.

(2) In the interpretation of this Act, regard is to be made to its international origin and need to promote harmonisation and uniformity in its application, as well as the observance of good faith.

(3) Any legal issues for which no specific provisions are laid down in this Act shall be governed in accordance with the international law principles, general principles of civil and commercial practice, customary law applicable in this country.

PART II. – JURISDICTION.

2. APPLICATION.

(1) This Act applies to any kind of data message and electronic document used in the context of commercial and non-commercial activities including domestic and international dealings, transactions, arrangements, agreements, exchanges and storage of information.

(2) This Act does not override any legal provision of the *Independent Consumer and Competition Commission Act* 2002 intended for the protection of consumers.

3. EXCLUSIONS.

This Act does not apply to-

(*a*) transactions on a regulated exchange; and
(*b*) foreign exchange transactions; and
(*c*) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; and
(*d*) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary; and
(*e*) transactions and issues relation to personal law such as marriages, divorce, the creation or execution of a will or any other testamentary disposition; and
(*f*) a Power-of-Attorney; and
(*g*) a trust, excluding a constructive, implied and resulting trust; and
(*h*) any deeds of title to immovable property (transactions involving the sale, purchase, lease and other disposition of immoveable property and the registration of other rights relating to immovable property); and
(*i*) any document legally required to be attested before a notary public (including affidavits, statutory declarations, or other documents involving an oath or affirmation); and
(*j*) any other documents or transactions exempted by special provisions of a law.

PART III. – ELECTRONIC TRANSACTIONS.

Division 1: Applicable principles.

4. PARTY AUTONOMY.

(1) Nothing in this Act requires a party to use or accept electronic records, but a party's agreement to do so may be inferred from the party's conduct.

(2) The provisions of this Act may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

5. LOCATION OF THE PARTIES.

(1) For the purposes of this Act, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

(2) If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this Act is that which has the closest relationship to the underlying transaction.

(3) For determination of a party location regard should be made to the circumstances known to or contemplated by the parties at any time before or at the time of carrying out that transaction or, where there is no underlying transaction, the principal place of business.

(4) If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

(5) A location is not a place of business merely because that is-

(*a*) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(*b*) where the information system may be accessed by other parties.

(6) The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

6. INFORMATION REQUIREMENTS.

Nothing in this Act affects the application of any legal provision that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate, incomplete or false statements in that regard.

Division 2: Legal effect, validity and enforceability of electronic records.

7. LEGAL RECOGNITION OF ELECTRONIC RECORDS.

(1) For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic record.

(2) Any information shall not be denied legal effect, validity or enforceability on the ground that the information is not contained in the electronic message that gives rise to such legal effect, but is merely referred to in that electronic message.

(3) Such referred in the electronic message information should be accessible to the person against whom the referred information might be used.

8. REQUIREMENT FOR WRITING.

(1) Subject to Subsection (2) where the law requires information to be written, in writing, to be presented in writing and provides for certain consequences if it is not, that requirement is met by a data message if the information contained in it is accessible so as to be usable for subsequent reference.

(2) Subsection (1) applies whether the requirement therein is in the form of an obligation not being in writing.

9. ORIGINAL.

(1) Subject to Subsection (2) where the law requires information to be presented or retained in its original form, that requirement is met by a data message if-

(*a*) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(*b*) where it is required that information be made available, that information is capable of being displayed to the person to whom it is to be made available.

(2) Subsection (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of Subsection (1)(*a*)-

(*a*) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(*b*) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Division 3: Various actions in relation to data messages.

10. ADMISSIBILITY AND EVIDENTIAL WEIGHT OF DATA MESSAGES.

The rules on electronic evidence set forth in the *Evidence (Amendment) Act* 2016 shall apply.

11. RETENTION OF DATA MESSAGES.

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied-

(*a*) the information contained therein is accessible so as to be usable for subsequent reference; and

(*b*) the data message 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*) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with Subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in Subsection (1) by using the services of any other person, provided that the conditions set forth in Subsection (1)(*a*), (*b*) and (*c*) are met.

12. RECOGNITION BY PARTIES OF DATA MESSAGES.

As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

13. ATTRIBUTION OF DATA MESSAGES.

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent-

(*a*) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(*b*) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if-

(*a*) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(*b*) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Subsection (3) does not apply-

(*a*) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(*b*) in a case within Subsection (3)(*b*), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the

originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption.

(6) The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(7) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption.

(8) Exceptions for that are duplication messages, when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

14. TIME AND PLACE OF DISPATCH AND RECEIPT OF DATA MESSAGES.

(1) Unless otherwise agreed between the originator and the addressee, the time of dispatch of a data message is 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.

(2) If the data message has not left immediately (meaning any time interval) an information system under the control of the originator or of the party who sent it on behalf of the originator, the reference should be to the time when the data message is received.

(3) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(4) The time of receipt of a data message at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the data message has been sent to that address.

(5) A data message is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(6) A data message is 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, as determined in accordance with Section 6.

(7) Subsection (2) applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the data message is deemed to be received under Subsection (3).

15. ACKNOWLEDGEMENT OF RECEIPT.

(1) Subsections (2) and (4) apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by-

(*a*) any communication by the addressee, automated or otherwise, or

(*b*) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator-

(*a*) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(*b*) if the acknowledgement is not received within the time specified in paragraph (*a*), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this section is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

PART IV. – ELECTRONIC CONTRACTING.

Division 1. Non-discrimination against electronic means in relation to contracts.

16. FORMATION AND VALIDITY OF CONTRACTS.

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic communications.

(2) Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic communication was used for that purpose.

17. INVITATIONS TO MAKE OFFERS.

(1) A proposal to conclude a contract can be 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.

(2) Such proposals that make use of interactive applications for the placement of orders through the information systems, are to be considered as invitations to make offers, unless it

clearly indicated that the intention of the party making the proposal is to be bound in case of acceptance.

Division 2. Specificities of contracts concluded with electronic means.

18. USE OF AUTOMATED MESSAGE SYSTEMS FOR CONTRACT FORMATION.

A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

19. AVAILABILITY OF CONTRACT TERMS.

Nothing in this Act affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those electronic communications which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

20. ERROR IN ELECTRONIC COMMUNICATIONS.

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

(*a*) the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(*b*) the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.

(2) Nothing in this Section affects the application of any rule of law that may govern the consequences of any error other than as provided for in Subsection (1).

21. ADDITIONAL INFORMATION.

Nothing in this Act precludes the inclusion of information in an electronic record, electronic communication or electronic transferable record in addition to that contained in a paper-based document or in a transferable document or instrument.

PART V. – ELECTRONIC SIGNATURES.

Division 1. Principles applicable to electronic signatures.

22. EQUAL TREATMENT OF SIGNATURE TECHNOLOGIES

Nothing in this Act, unless principle of party autonomy, as described in Section 4, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in Section 23(1), or otherwise meets the requirements of applicable law.

23. ELECTRONIC SIGNATURES.

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Subsection (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in Subsection (1) if-

(*a*) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; and

(*b*) the signature creation data were, at the time of signing, under the control of the signatory and of no other person; and

(*c*) any alteration to the electronic signature, made after the time of signing, is detectable; and

(*d*) where a 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 detectable.

(4) Subsection (3) does not limit the ability of any person-

(*a*) to establish in any other way, for the purpose of satisfying the requirement referred to in Subsection (1), the reliability of an electronic signature; or

(*b*) to adduce evidence of the non-reliability of an electronic signature.

24. TRUSTWORTHINESS.

For the purposes of Section 27(1)(*f*), this Act in determining whether, or to what extent, any systems, procedures and human resources utilized by a service provider are trustworthy, regard may be had to the following factors-

(*a*) financial and human resources, including existence of assets; or

(*b*) quality of hardware and software systems; or

(*c*) procedures for processing electronic signatures and applications for electronic signatures and retention of records; or

(*d*) availability of information to signatories identified in electronic signatures and to potential relying parties; or

(*e*) regularity and extent of audit by an independent body; or

(*f*) the existence of a declaration by an accreditation body or the service provider regarding compliance with or existence of the foregoing; or

(*g*) any other relevant factor.

25. RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES.

(1) In determining whether, or to what extent, an electronic signature is legally effective, no regard shall be had-

(*a*) to the geographic location where the electronic signature is created or used; or

(*b*) to the geographic location of the place of business of the issuer or signatory.

(2) An electronic signature created or used outside Papua New Guinea shall have the same legal effect in Papua New Guinea as an electronic signature created or used in Papua New Guinea if it offers a substantially equivalent level of reliability.

(3) In determining whether an electronic signature offers a substantially equivalent level of reliability for the purposes of Subsection (2) regard shall be had to recognized international standards and to any other relevant factors.

(4) Where, notwithstanding Subsections (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures, 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.

Division 2. Conduct of signatory, service provider and relying party.

26. CONDUCT OF THE 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; and

(*b*) without undue delay, utilize means made available by the service provider pursuant to Section 27(1)(*d*)(*v*) of this Act, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or 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.

(2) 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 certificate.

(3) A signatory shall bear the legal consequences of its failure to satisfy the requirements of Subsection (1).

27. CONDUCT OF THE SERVICE PROVIDER.

(1) Where a service provider provides services to support an electronic signature that may be used for legal effect as a signature, that service provider shall-

(*a*) act in accordance with representations made by it with respect to its policies and practices; and

(*b*) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the electronic signature throughout its life cycle or that are included in the electronic signature; and

(*c*) provide reasonably accessible means that enable a relying party to ascertain from the electronic signature:-

(i) the identity of the service provider; and

(ii) that the signatory that is identified in the electronic signature had control of the signature creation data at the time when the electronic signature was issued; and
(iii) that signature creation data were valid at or before the time when the electronic signature was issued; and

(*d*) provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the electronic signature or otherwise:-
(i) the method used to identify the signatory; and
(ii) any limitation on the purpose or value for which the signature creation data or the electronic signature may be used; and
(iii) that the signature creation data are valid and have not been compromised; and
(iv) any limitation on the scope or extent of liability stipulated by the service provider; and
(v) whether means exist for the signatory to give notice pursuant to Subsection (1)(*b*) of this Act; and
(vi) whether a timely revocation service is offered; and
(*e*) where services under Subsection (1)(*d*)(v) are offered, provide a means for a signatory to give notice pursuant to Subsection (1)(*b*), of this Act and, where services under Subsection (1)(*d*)(vi) are offered, ensure the availability of a timely revocation service; and
(*f*) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A service provider shall bear the legal consequences of its failure to satisfy the requirements of Subsection (1).

28. CONDUCT OF THE RELYING PARTY.

A relying party shall bear the legal consequences of its failure-
(*a*) to take reasonable steps to verify the reliability of an electronic signature; or
(*b*) where an electronic signature is supported by a certificate, to take reasonable steps:-
(i) to verify the validity, suspension or revocation of the certificate; and
(ii) to observe any limitation with respect to the certificate.

PART VI. - ELECTRONIC TRANSFERABLE RECORDS.

Division 1. Principles applicable to electronic transferable records.

29. ELECTRONIC TRANSFERABLE RECORDS.

(1) This Part applies to electronic transferable records.

(2) Other than as provided for in this Act, nothing in this Act 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.

(3) This Part does not apply to securities, such as shares and bonds, and other investment instruments.

30. LEGAL RECOGNITION OF AN ELECTRONIC TRANSFERABLE RECORD.

An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form.

31. 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; and

(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.

32. NON-DISCRIMINATION OF FOREIGN ELECTRONIC TRANSFERABLE RECORDS.

(1) An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it was issued or used abroad.

(2) Nothing in this Part affects the application to electronic transferable records of rules of private international law governing a transferable document or instrument.

Division 2. Control necessary in relation to electronic transferable records.

33. CONCEPT OF 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.

34. GENERAL RELIABILITY STANDARD.

For the purposes of Sections 31, 33, 35, 37, 38 and 39, the method referred to shall be-

(*a*) as reliable as appropriate for the fulfilment of the function for which the method is being used, in light of all relevant circumstances, which may include:-

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

(ii) the assurance of data integrity; or

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

(iv) the security of hardware and software; or

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

(vi) the existence of a declaration by a supervisory body, 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.

Division 3. Time, place, amendments and endorsement of electronic transferable records.

35. 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.

36. 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 sections in relation to writing and electronic signatures.

37. 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.

Division 4. Replacements of transferable documents.

38. 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 Subsections (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 Subsections (1) and (2) shall not affect the rights and obligations of the parties.

39. 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 Subsections (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 Subsections (1) and (2) shall not affect the rights and obligations of the parties.

PART VII. - MISCELLANEOUS.

40. EXTENT OF LIABILITY OF A SERVICE PROVIDER.

(1) Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of the electronic data message or electronic document for which the person or party acting as a service provider merely provides access if such liability is founded on-

(*a*) the obligations and liabilities of the parties under the electronic data message or electronic document; and

(*b*) the making, publication, dissemination or distribution of such material or any statement made in such material, including possible infringement of any right subsisting in or in relation to such material, provided that:-

(i) the service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material; and

(ii) the service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and

(iii) the service provider does not directly commit any infringement or other unlawful act and does not induce or cause another person or party to commit any infringement or other unlawful act and/or does not benefit financially from the infringing activity or unlawful act or another person or party.

(2) Nothing in this Section shall affect-

(*a*) any obligation founded on contract; or

(*b*) the obligation of a service provider as such under a licensing or other regulatory regime established under written law; or

(*c*) any obligation imposed under any other law; or

(*d*) the civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any material, or to preserve evidence of a violation of law.

41. LAWFUL ACCESS.

(1) Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of plaintext, electronic signature or file or solely for the authorized purposes.

(2) The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.

42. OBLIGATION OF CONFIDENTIALITY.

Except for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.

43. PENALTIES.

The Regulations may provide for the penalties that may be imposed under this Act.