BELIZE:

ELECTRONIC TRANSACTIONS BILL, 2021

ARRANGEMENT OF SECTIONS

PART VII

Electronic Transferable Records

PART VIII

Information Security Procedures Providers

PART IX

Digital Government

BELIZE:

BILL

AN ACT to give legal effect to all electronic documents, records and signatures; to repeal the Electronic Transactions Act, Chapter 229:03 of the Substantive Laws of Belize, Revised Edition 2011; and to provide for matters connected therewith or incidental thereto.

(Gazetted ....., 20.....)

BE IT ENACTED, by and with the advice and consent of the House of Representatives and Senate of Belize and by the authority of the same, as follows:

PART I

Preliminary

Short title

1. This Act may be cited as the

ELECTRONIC TRANSACTIONS ACT, 2021.

Objects.

2. The objects of this Act are to facilitate the use of all electronic communications in the public and private sectors and to better promote the harmonisation of legal rules on electronic transactions to electronic documents, records and signatures.

Interpretation.

3. In this Act, unless the context otherwise requires–

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

"authentication data" includes user name, password and license key;

"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 an individual each time an action is initiated or a response is generated by the program or electronic or other means;

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

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

"Court" means the Supreme Court of Belize;

"digital signature" means a signature that fulfills the requirements of section 26;

"electronic" includes electrical, digital, magnetic, wireless, optical, electro-magnetic, biometric, photonic and similar capabilities;

"electronic-commerce service provider" means a person who uses electronic means in providing goods or services or both;

"electronic communication" means information which is communicated, processed, recorded, displayed, created, stored, generated, received or transmitted in an electronic form;

"electronic form," with reference to information, means any information generated, sent, received or stored in media, magnetic form, optical form, computer memory, microfilm, computer generated microfiche or similar device;

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

"electronic transferable record" means an electronic record that complies with the requirements of section 33;

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

"enterprise" means a partnership or body, whether corporate or unincorporated, engaged in business;

"individual" means a natural person;

"information" includes data, text, documents, images, sounds, codes, computer programmes, software and databases;

"information system" means a system for generating, sending, receiving, storing or otherwise processing an electronic record;

"intermediary", with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives, transmits or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes telecommunication service providers, network service providers, Internet service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafés;

"Minister" means the Minister to whom responsibility for e-government and Electronic Commerce is assigned;

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

"public authority" means any Ministry, department, agency, board, commission, local democratic organ or other body of the Government and includes an entity or body established by law or by arrangement of the Government or a Minister for a non-commercial public service purpose;

"record" means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

"security procedure" means a procedure established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, communication or performance is that of a particular person or for detecting changes or errors in content of an electronic communication;

'signatory' means an individual who creates an electronic signature;

"signature creation data" means unique data, including codes or private cryptographic keys or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

"signed" or "signature" and its grammatical variations mean a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record;

"specified security procedure" means a security procedure which is specified by Order by the Minister;

"specified security procedure provider " means a person involved in the provision of a specified security procedure.

“time stamp” means a data unit created using a system of technical and organisational means which certifies the existence of electronic data at a given time;

“transaction” means an action or set of actions relating to the conduct of business, consumer or commercial affairs between two or more persons including the sale, lease, exchange, licensing or other disposition of personal property, including goods and intangible interests in real property, services or any combination of any of these acts;

“transferable document or instrument” mean a document or instrument issued on paper that entitles the holder to–

(a) claim the performance of the obligation indicated in the document or instrument; and

(b) transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.

(2) In this Act, “place of business”, in relation to a party, means–

(a) any place where the 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; or

(b) if the party is a individual and he does not have a place of business, the person’s habitual residence.

(3) For the purposes of sub-section (2)–

(a) if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;

(b) if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;

(c) a location is not a place of business merely because that location is–

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

(ii) where the information system may be accessed by other parties; and

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

(4) Where an electronic communication does not relate to any contract, references to a contract in sub-section (3) shall refer to the relevant transaction.

Purposes and construction.

4.–(1) This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes–

(a) to provide for the development, promotion and facilitation of electronic transactions and related electronic communications;

(b) to remove and prevent barriers to electronic transactions and related electronic communications including in all enactments except where specifically excluded;

(c) to promote legal certainty and confidence in electronic transactions and electronic communications;

(d) to promote e-government services and electronic commerce and electronic communications with, by, between and for public and private bodies, institutions and individuals;

(f) to promote the development of electronic transaction services responsive to the needs of consumers;

(g) to ensure that, in relation to the provision of electronic transactions and services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account;

(h) to ensure compliance with accepted international technical standards in the provision and development of electronic transactions and related electronic communications; and

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

Autonomy of Parties.

5.–(1) Nothing in this Act shall prohibit any person engaging in a transaction through the use of electronic means from establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

(2) A transaction which has been conducted using electronic means shall not be denied legal effect, validity or enforceability solely for the reason of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

State to be bound.

6. This Act binds the State.

PART II

Requirements for Legal Recognition

Legal recognition of electronic communications.

7. An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is–

(a) rendered or made available in electronic form; or

(b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication.

Requirement to provide information in writing.

8.–(1) Where any information or other matter is required by any law to be given or rendered in writing, recorded in writing or in printed form, or is described as being written, notwithstanding anything contained in the law, the requirement or description, shall be deemed to be satisfied if the information or matter is–

(a) rendered, recorded or made available in electronic form; and

(b) accessible to, and is capable of retention by, the intended recipient so as to be usable or retrievable for a subsequent reference.

(2) Sub-section (1) shall apply whether the requirement for the information to be, in writing or recorded in writing, is in the form of an obligation or the law provides consequences if it is not in writing.

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

(4) Where any information is retained in electronic form in accordance with sub-section (1), and is retrievable at any time during the specified period of retention, the paper or other non-electronic form of that information need not be retained.

Requirement to provide access to information in paper form.

9. A legal requirement to provide access to information that is in paper or other non-electronic form, is satisfied by providing access to the information in electronic form where the form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided.

Delivery of information.

10.–(1) Where information is required by law to be delivered, dispatched, given or sent to, or be served on a person, the requirement is met by doing so in the form of an electronic record, provided that the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee has acknowledged its receipt.

(2) Sub-section (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

Information in original form.

11.–(1) Where information is required by law to be presented or retained in its original form, the requirement is met by an electronic communication 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 as an electronic communication or otherwise; and

(b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

(2) Sub-section (1) shall apply whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of sub-section (1)*(a)*–

(a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the additions of any endorsement and any change which arises in the normal course of communication, storage and display; and

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

Retention of documents, records or information in electronic form.

12.–(1) Where certain documents, records or information are required by law to be retained in paper or other non-electronic form, that requirement is met by retaining it in electronic form if the following conditions are satisfied–

(a) the information contained in electronic form is accessible so as to be usable for subsequent reference;

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

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

(2) An obligation to retain documents, records or information in accordance with sub-section (1)*(c)* shall not apply 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 under sub-section (1) by using the services of any other person, if the conditions set out in sub-section (1) are met.

(4) Nothing in this section shall preclude any public authority from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of the public authority.

Other requirements.

13.–(1) An expression in a law, whether used as a noun or verb, including the terms “document", "record", "file", "submit", "lodge", "deliver", "issue",

"publish", "write in", "print" “register” or words or expressions of similar effect, shall be interpreted so as to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

(2) Where a seal is required by any law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed, that requirement shall be met if the document indicates that–

(a) it is required to be under seal and includes the digital signature of the person by whom it is required to be sealed; or

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

(3) Where information, a signature, document or record is required by any law, rule of law, by contract or deed to be notarised, apostilled, acknowledged, verified or made under oath, the requirement shall be satisfied if, in relation to an electronic signature, electronic document or electronic record, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the electronic signature, electronic document or electronic record.

Comparison of documents with original.

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

Admissibility of electronic records.

15. In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied solely on the grounds that it is an electronic record or an electronic signature.

PART III
Electronic Contracts

Formation and validity of contracts.

16.–(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts, an offer and the acceptance of an offer may be given 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 solely on the ground that an electronic communication was used for that purpose.

Effectiveness between parties.

17. As between the originator and the addressee of an electronic communication, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic communication.

Time and place of dispatch and receipt of electronic communications.

18.–(1) The time of dispatch of an electronic communication is–

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

(b) if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

(4) For the purposes of sub-section (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

(5) An electronic communication 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.

(6) Sub-sections (2), (3) and (4) shall apply notwithstanding that the place where the information system supporting an electronic address is located, is different from the place where the electronic communication is deemed to be received under sub-section (5).

Invitation to make offer.

19. 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 a proposal that uses interactive applications for the placement of orders through the information systems, shall 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.

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

Use of automated message systems for contract formation.

21.–(1) Where an individual 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.

Error in electronic communications.

(2) Sub-section (1) shall not apply unless the person, or the party on whose behalf that person was acting–

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

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

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

PART IV

Electronic Signatures

22. Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record.

Requirement for signature.

23. Unless otherwise provided by law, the parties to an electronic transaction may agree to the use of a particular method or form of electronic signature or security procedure.

Equal treatment of signatures.

24.–(1) In determining whether, or the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.

Recognition of foreign certificates and electronic signatures.

(2) Where the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be sufficient for the purpose of cross-border recognition in respect of that transaction.

PART V

Digital Signatures

Conduct of the signatory.

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

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

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

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

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

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

Digital signature.

26. Where, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made–

(a) unique to the person using it;

(b) capable of identifying the person using it;

(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 changed the electronic signature would be invalidated,

such signature shall be treated as digital signature.

Presumptions relating to digital records and signatures.

27. In any proceedings involving a digital signature, it shall be presumed, unless evidence to the contrary is adduced, that–

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

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

PART VI

Electronic time stamps

Legal effect of electronic time stamps.

28.–(1) An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.

(2) A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

Requirements for qualified electronic time stamps.

29.–(1) A qualified electronic time stamp shall meet the following requirements–

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

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

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

(3) Compliance with the requirements laid down in regulations made under sub-section (1) shall be presumed where the binding of date and time to data and the accurate time source meets those standards.

PART VII

Electronic Transferable Records

Application of this Part.

30.–(1) Other than as provided for in this Act, nothing in this Part 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.

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

Additional information in electronic transferable records.

31. Nothing in this Act precludes the inclusion of information in an electronic transferable record in addition to that contained in a transferable document or instrument.

General reliability standard.

32.–(1) For the purposes of this Part, a method shall be deemed reliable if it is–

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

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

(ii) the assurance of data integrity;

(iii) the ability to prevent 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; or

(vii) any applicable industry standard; or

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

Legal requirement for transferable documents or instruments.

33.–(1) A rule of law that requires a transferable document or instrument is met by a data message if–

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

(b) a reliable method is used to–

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

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

(iii) retain the integrity of that data message.

(2) For the purposes of sub-section (1)*(b)(iii)*, 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.

Control.

34.–(1) Any rule of law that requires or permits the possession of a transferable document or instrument is met with respect to an electronic transferable record if a reliable method is used to–

(a) establish exclusive control of that electronic transferable record by a person; and

(b) identify that person as the person in control.

(2) A rule of law that requires or permits transfer of possession of a transferable document or instrument is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

Indication of time and place in electronic transferable record.

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

Endorsement.

36. A rule of law that requires or permits the endorsement in any form of a transferable document or instrument 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 8 and 22.

Amendment.

37. A rule of law that requires or permits the amendment of a transferable document or instrument 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.

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

38.–(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 this section, 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 this section shall not affect the rights and obligations of the parties.

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

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

(a) a reliable method for the change of medium is used; and

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

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

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

Non-Discrimination of foreign electronic transferable records.

40.–(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.

PART VIII

Information Security Procedures Providers

Specified security procedure providers.

41. The Minister may, by Order, list the classes of specified security procedure providers to which this section applies.

Regulation of specified security procedure and specified security procedure providers.

42.–(1) The Minister may make regulations, for the carrying out of this Act and, without prejudice to the general power, for any of the following purposes–

(a) regulating, registering, licensing or accreditation of specified security procedure providers and their authorised representatives;

(b) safeguarding or maintaining the effectiveness and efficiency of the common security infrastructure relating to the use of digital signatures and the authentication of electronic records, including the imposition of requirements to ensure interoperability between specified security procedure providers or in relation to any security procedure;

(c) ensuring that the common security infrastructure relating to the use of digital signatures and the authentication of electronic records, is in compliance with Belize's international obligations; or

(d) prescribing the forms and fees applicable for the purposes of this Part.

(2) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties of a fine not exceeding $50,000 or imprisonment for a term not exceeding 12 months or both.

PART IX

Digital Government

Use of electronic records and electronic signatures in Government and its agencies.

43.–(1) Any public authority that, pursuant to any written law–

(a) accepts the filing of documents, or obtains information in any form;

(b) requires that documents be created or retained;

(c) requires documents, records or information to be provided or retained in their original form;

(d) issues any permit, licence or approval; or

(e) requires payment of any fee, charge or other amount by any method and manner of payment,

may, notwithstanding anything to the contrary in such written law, carry out such function by means of electronic records or in electronic form.

(2) In any case where a public authority performs a function under sub-section (1), by means of electronic records or in electronic form, the public authority may specify–

(a) the manner and format in which the electronic records shall be filed, created, retained, issued or provided;

(b) where the electronic records is to be signed, the type of electronic signature required, including, if applicable, a requirement that the sender of the record use a particular type of digital 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; or

(e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under sub-section (2), where any person is required by any written law to perform a function mentioned under sub-section (4), such requirement shall be satisfied by an electronic record specified by the public authority for that purpose.

(4) The functions referred to under sub-section (3), include–

(a) file any document with, or provide information in any form to, a public authority;

(b) create or retain any document for a public authority;

(c) use a prescribed form for an application or notification to, or other transaction with, a public authority;

(d) provide to or retain for a public authority, any document, record or information in its original form; or

(e) hold a licence, permit or other approval from a public authority,

(5) A requirement under sub-section (4) shall–

(a) in the case of a requirement under sub-paragraph *(a)*, *(c)* or *(d)*, be transmitted or retained, as the case may be, in the manner specified by the public authority;

(b) in the case of a requirement referred under sub-paragraph *(b)*, be created or retained, as the case may be, in the manner specified by the public authority; or

(c) in the case of a requirement referred to in sub-paragraph *(e)*, be issued by the public authority.

Records available for inspection.

44. Where documents, records or information are required by any statutory provision or rule of law, contract or by deed to be made available for inspection , the requirement shall be met by making such documents, records or information available for inspection as an electronic record.

Furnishing of information in prescribed forms.

45. Notwithstanding anything contained in any law, a legal requirement that a person provide information in a prescribed paper or other non-electronic form to another person is satisfied by providing the information in an electronic form that–

(a) contains the same or substantially the same information as the prescribed paper or other non-electronic form;

(b) is accessible to the other person so as to be usable or retrievable for subsequent reference; and

(c) is capable of being retained by the other person.

PART X

Intermediaries and Electronic Commerce Service Providers

Liabilities of intermediaries.

46.–(1) An intermediary or electronic commerce service provider shall not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary

provides services, if the intermediary was not the originator of the record and the intermediary or electronic commerce service provider–

(a) has no actual knowledge that the information that gave rise to civil or criminal liability;

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or

(c) follows the procedure set out in section 47 if the intermediary or electronic commerce service provider–

(i) acquires knowledge that the information gives rise to criminal liability; or

(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary or electronic commerce service provider shall not be required to monitor any electronic record processed by means of his system in order to ascertain whether its processing would (apart from this section) constitute or give rise to an offence or give rise to civil liability.

(3) Nothing in this section shall relieve an intermediary or electronic commerce service provider from–

(a) any obligation to comply with an order or direction of a court or other competent authority; or

(b) any contractual obligation.

Procedure for dealing with unlawful information.

47.–(1) Where an intermediary or electronic commerce service provider has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, as soon as practicable, the intermediary or electronic commerce service provider shall–

(a) remove the information from any information system within the intermediary's or electronic commerce service provider's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the Minister or appropriate law enforcement authority in writing of the relevant facts and of the identity of the person for whom the intermediary or electronic commerce service provider was supplying services in

respect of the information, if the identity of that person is known to the intermediary or electronic commerce service provider.

(2) If an intermediary or electronic commerce service provider is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic record ought reasonably to have been known, as soon as practicable the intermediary or electronic commerce service provider shall–

(a) follow the relevant procedure set out in a code of conduct approved or standard appointed under this Act if such code or standard applies to the intermediary or electronic commerce service provider; or

(b) notify the Minister in writing .

(3) Where the Minister is notified in respect of any information under sub-section (2), the Minister may direct the intermediary or electronic commerce service provider to–

(a) remove the electronic record from any information processing system within the control of the intermediary or electronic commerce service provider;

(b) cease to provide services to the person to whom the intermediary or electronic commerce service provider was supplying services in respect of that electronic record; and

(c) cease to provide services in respect of that electronic record.

(4) An intermediary or electronic commerce service provider shall not be liable, whether in contract, tort, under statute or pursuant to any other right, to any person, including any person on whose behalf the intermediary or electronic commerce service provider provides services in respect of information in an electronic record, for any action the intermediary or electronic commerce service provider takes in good faith in exercise of the powers conferred by, or as directed by, the Minister, under this section.

(5) Any person who lodges a notification of unlawful activity with an intermediary or electronic commerce service provider, knowing that it materially misrepresents the facts, commits an offence and is liable for damages for wrongful removal of the information or electronic record under sub-sections (1) to (3).

(6) Where a code of conduct is approved or a standard is specified by the Minister under this Act to apply to intermediaries or electronic-commerce service providers, the intermediaries or electronic-commerce service

providers shall comply with the code of conduct or standards, as the case may be.

Codes of conduct and standards for intermediaries and electronic commerce service providers.

48.–(1) Where a code of conduct is approved or a standard is specified by the Minister under this section to apply to intermediaries or electronic-commerce service providers, those intermediaries or electronic-commerce service providers shall comply with the code of conduct or standards, as the case may be.

(2) An intermediary or electronic-commerce service provider who fails to comply with an approved code of conduct or specified standard, shall in the first instance be issued a written warning by the Minister and the Minister may, , direct that intermediary or electronic-commerce service provider, in writing, to cease and desist or otherwise to correct his practices.

(3) An intermediary or electronic-commerce service provider who fails comply with a direction under sub-section (2), within the period specified in the direction, commits an offence and is liable on summary conviction to a fine of fifty thousand dollars for the first offence and to a fine of one thousand dollars for each subsequent offence for each day the offence continues.

(4) Where the Minister is satisfied that a body or organisation represents intermediaries or electronic-commerce service providers, the Minister may, by notice given to the body or organisation, direct the body or organisation to–

(a) develop a code of conduct that applies to intermediaries or electronic-commerce service providers who deal with one or more specified matters relating to the provision of services by those intermediaries or electronic-commerce service providers; and

(b) submit a copy of the code of conduct to the Minister within such time as may be specified in the direction.

(5) Where the Minister is satisfied with the code of conduct submitted under sub-section (4), the Minister shall approve the code of conduct by notice published in the Gazette and thereupon the code of conduct shall apply to intermediaries or electronic-commerce service providers, as the case may be, as specified in the notice.

(6) The Minister may, by notice published in the Gazette, revoke or amend the existing code of conduct or standard, as the case may be.

PART XI

Consumer Protection

Minimum information in Electronic Commerce.

49.–(1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves including the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number, sufficient to allow–

(a) prompt, easy and effective consumer communication with the seller; and

(b) service of legal process.

(2) A person using electronic communications to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information.

(3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction, including–

(a) terms, conditions and methods of payment; and details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information; and

(b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

PART XII

Contravention and Enforcement

False or misleading information.

50. A person commits and offence under this Act if that person–

(a) files information required under this Act that contains false or misleading information;

(b) provides a consumer or a user of an electronic signature with false or misleading information.

Penalties.

51.–(1) A person who commits an offence under this Act for which no penalty is provided is liable–

(a) upon summary conviction to a fine of [two hundred thousand dollars] or to imprisonment for a term of three years, or to both fine and imprisonment; and

(b) upon conviction on indictment to a fine of [two hundred and fifty thousand dollars] or to imprisonment for a term of five years or to both fine and imprisonment.

(2) Where an offence under this Act is committed by a body corporate for which no penalty is provided, the body corporate is liable–

(a) on summary conviction to a fine of two hundred and fifty thousand dollars; and

(b) on conviction on indictment to a fine of five hundred thousand dollars.

(3) Where an enterprise contravenes any of the provisions of this Act the Court may, in addition to any penalty it may impose for a criminal offence, impose a fine up to ten per cent of the annual turnover of the enterprise.

(4) In imposing a fine under sub-section (3) the Court shall take into account–

(a) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;

(b) the estimate of the economic benefit of the contravention to the enterprise;

(c) the time for which the contravention is in effect if continuing;

(d) the number and seriousness of any other contraventions, if any, committed by the enterprise; and

(e) any other matter the Court considers appropriate in the circumstances.

PART XIII

Miscellaneous

Cloud services.

52.–(1) Notwithstanding anything contained in any other enactment, a Public Authority may contract a third party to provide cloud services.

(2) The Minister may make Regulations for the purpose of contract entered into under sub-section (1) including specifying requirements on proper use, confidentiality, data location and transfer, access by the provider, rights over service and contents, liability, warranty, auditing requirements, cloud-computing institution overseers, and performance management.

Exceptions.

53.–(1) This Act shall not apply to any written law requiring writing, signatures or original documents that may be determined by the Minister by Order.

(2) Electronic documents with dispositions of real estate shall be signed using digital signature.

Regulations.

54. The Minister may make Regulations for the purpose of giving effect to this Act.

Conflict of enactments.

55. Where there is any conflict between the provisions of this Act and any other relevant enactment, the provisions of this Act shall prevail to the extent of the inconsistency.

Repeal. CAP. 229:03.

56. The Electronic Transactions Act is repealed.