A BILL
for
AN ACT TO PROVIDE FOR THE LEGAL RECOGNITION OF ELECTRONIC WRITING, ELECTRONIC CONTRACTS, ELECTRONIC SIGNATURES AND ORIGINAL INFORMATION IN ELECTRONIC FORM IN RELATION TO COMMERCIAL AND OTHER TRANSACTIONS AND TO PROVIDE FOR THE FACILITATION OF ELECTRONIC TRANSACTIONS AND RELATED MATTERS.

PART I
PRELIMINARY

Short title and commencement

(1) (1) This Act may be cited as the E-Commerce Act, 2003.

(2) This Act shall come into operation on such day as the Minister may, by notice published in the Gazette, appoint.

Definitions

2. In this Act -

“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;

“consumer” means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes;

“e-commerce service provider” means a person who uses electronic means in providing goods and services;

“electronic” means relating to technology and having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

“electronic authentication” means any procedure employed for the purpose of verifying that an electronic communication is that of the originator and that it has not been altered during transmission;

“electronic agent” means a program, or other electronic or automated means that is used independently to initiate or respond to electronic communications or performances in whole or in part without review by an individual;

“electronic communication” means information which is communicated, processed, recorded, displayed, created, stored, generated,

received or transmitted by electronic means;

"electronic signature" means any letters, characters, numbers, sound, process or symbols in electronic form attached to, or logically associated with information that is used by a signatory to indicate his intention to be bound by the content of that information;

"host" means a person who provides a service that consists of the storage in electronic form of information provided by another person;

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

"information processing system" means an electronic system for creating, generating, sending, receiving, recording, storing, displaying, or otherwise processing information;

"information security service" and "information security procedure" includes a service or procedure which is provided to an originator, intermediary, or recipient of an electronic record, and which is designed to –
(a) secure that that record can be accessed, or can be put into an intelligible form, only by certain persons; or
(b) secure that –
(i) the authenticity;
(ii) the time of processing; or
(iii) the integrity,
of such a record is capable of being ascertained.

"intermediary" with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives or stores either temporary or permanently that electronic communication or provides related services with respect to that electronic communication;

"Minister" means the Minister with responsibility for Electronic Commerce;

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

"prescribed" means prescribed by regulations under section 31;

"public body" means any Ministry, agency, board, commission or other body of the Government and includes an entity or body established by

law, or by arrangement of the Government or a Minister of the Government 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;

"signed" or "signature" includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic methods;

"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 intangibles, interest in real property, services, or any combination of the foregoing.

Crown to be bound

3. (1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act obliges any public body to generate, send, receive, store or otherwise process any record by electronic means, but the Minister may, by notice published in the Gazette, indicate that a public body may receive and process electronic communications relating to such matters as may be specified in the notice.

Exclusions

4. Part II shall not apply to any rule of law requiring writing or signatures for the following-

a) the creation, execution, amendment, variation or revocation of –

(i) a will or testamentary instrument; or

(ii) a trust;

(b) the conveyance of real property or the transfer of any interest in real property;

(c) court orders or notices, or official court

documents required to be executed in connection with court proceedings;
(d) enduring powers of attorney to the extent that they concern the financial affairs or personal care of an individual;
(e) all other deeds and documents described in section 3 of the Registration of Records Act, not otherwise expressly provided for under this subsection.

Autonomy of parties

5. (1) Nothing in this Act shall -
(a) require any person to use or accept electronic communications, electronic signatures, or electronic contracts; or
(b) prohibit any person engaging in a transaction through the use of electronic means from -
(i) varying by agreement any provision relating to legal recognition and functional equivalency of electronic communications, signatures, and contracts specified in Part II; or
(ii) 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 because of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

Consumer consent to electronic communications

6. Notwithstanding section 7, if a statutory or legal requirement exists for a record to be provided in writing to a consumer, such requirement for writing shall be satisfied by an electronic communication only if -
(a) the consumer has expressly consented to such use and has not withdrawn his consent; and
(b) prior to consenting, the consumer is provided with a clear and conspicuous statement informing the consumer –
i) about the right to have the record provided in non-electric form;
(ii) about the right to withdraw consent to have the record provided in electronic form and of any conditions, consequences or fees in the event of such withdrawal;
(iii) whether the consent applies only to the

particular transaction which gave rise to the obligation to provide the record, or to identified categories of records that may be provided during the course of the parties' relationship;

(iv) of the hardware and software requirements for access to, and retention of, the relevant electronic record;

(v) of the procedures for withdrawal of consent and to update information needed to contact the consumer electronically; and

(vi) of the procedures, after consent has been given, for obtaining a paper copy of the electronic record and any fee to be charged in connection therewith.

PART II
LEGAL RECOGNITION AND FUNCTIONAL EQUIVALENCY OF ELECTRONIC COMMUNICATIONS, SIGNATURES, CONTRACTS AND RELATED MATTERS

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) 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.

Writing

8. (1) Where information is required by law either to be in writing or is described as being written, such requirement or description is met by an electronic communication if the information contained in the electronic communication is accessible to, and is capable of retention by, the intended recipient.

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

Original form

9. (1) Where information is required by law to be presented or retained in its original form, that 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) Subsection (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 subsection (1)(a) -
a) the criterion for assessing integrity is 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 is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

Retention of electronic communications

10. (1) Where certain documents, records or information are required by law to be retained, that requirement is met by retaining electronic communications if the following conditions are satisfied -
(a) the information contained in the electronic communication 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 subsection (1) shall 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, if the conditions set out in subsection (1)(a), (b) and (c) are met.
(4) Nothing in this section shall preclude any

public body from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of such public body.

Admissibility and evidential weight electronic communications

11. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic communication in evidence solely on the ground that of it is in electronic form.

2) Information in the form of an electronic communication will be given due evidential weight and in assessing the evidential weight of an electronic communication, regard shall be had to –

a) the reliability of the manner in which the electronic communication was generated, stored or transmitted;

(b) the reliability of the manner in which the integrity of the information was maintained;

(c) the manner in which the originator was identified; and

(d) any other relevant factor.

No.15 1996.

(3) This section shall not affect the application of sections 61 and 67 of the Evidence Act (which relates to the admissibility of documents produced by computers).

Formation and validity of contracts

12. In the context of formation of contracts, unless otherwise agreed by the parties, an offer and the . the acceptance of an offer may be expressed by means of electronic communications.

Attribution of electronic communications

13. (1) An electronic communication is attributable to a person if the electronic communication resulted from the action of the person, acting in person, by his agent, or by his electronic agent device.

(2) Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic communication was attributable.

(3) An addressee is not entitled to regard the electronic communication received as being what the originator intended to send where the addressee knew or ought reasonably to have known, had he exercised reasonable care or used an agreed procedure, that the transmission resulted in any error in the

electronic communication as received.

(4) Nothing in this section affects the law of agency or the law on the formation of contracts.

Acknowledgement of receipt of electronic communications

14. (1) Where the originator of an electronic communication has stated that the electronic communication is conditional upon receipt of an acknowledgement -

(a) the electronic communication is to be – treated as though it had never been sent until the acknowledgement is received;

(b) if there is no agreement between the originator and the addressee as to the particular form or method of the acknowledgement to be given, the addressee may give an acknowledgement by any means of communication automated or otherwise or by any conduct that is reasonably sufficient to indicate to the originator that the electronic communication has been received.

(2) Where the originator indicates that receipt of an electronic communication is required to be acknowledged but has not stated that the electronic communication 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 electronic communication as though it had never been sent or exercise any other rights the originator may have.

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

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

Delivery, etc.

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

(2) Subsection (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.

(3) Subject to subsection 5, the dispatch of an electronic communication occurs when it enters an information processing system outside the control of the originator.

(4) Subject to subsection 5, the time of receipt of an electronic communication is determined as follows –

(a) where the addressee has designated an information processing system for the purpose of receiving electronic communications, receipt occurs –

(i) at the time when the electronic communication enters the designated information processing system; or

(ii) if the electronic communication is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic communication comes to the attention of the addressee;

(b) where the addressee has not designated an information processing system, receipt is deemed to have occurred on the earlier happening of –

(i) the time at which the electronic communication enters an information processing system of the addressee; or

(ii) otherwise comes to the attention of the addressee.

(5) Subsection (4) shall apply notwithstanding that the place where the information processing system is located may be different from the place where the electronic communication is deemed to be received under subsection (6).

(6) Unless otherwise agreed between the originator and the addressee, an electronic

communication is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(7) For the purposes of subsection (6) –

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic communication relates or, where there is no such transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

Copyright.

16. (1) The generation of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

(2) The production, by means of an electronic communication, of an electronic form of a document for the purposes of this Part does not constitute an infringement of the copyright in a work or other subject matter embodied in the document.

PART III
INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

Liability of intermediaries

17. (1) An intermediary shall not be subject to any civil or criminal liability in respect of third-party information contained in an electronic communication for which such intermediary is only providing access and he -

(a) has no actual knowledge that the information gives 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 21 if the intermediary –

(i) acquires knowledge that the information gives

rise to civil or 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 shall not be required to monitor any information contained in an electronic communication in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

(3) Nothing in this section shall relieve an intermediary from complying with any court order, injunction, writ, Ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic communication.

(4) For the purposes of this section -

"provides access", in relation to third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing access;

"third-party information" means information of which the intermediary is not the originator.

Procedure for dealing with unlawful, defamatory etc.

18. (1) If an intermediary has actual knowledge that the information in an electronic communication gives rise to civil or criminal liability, as soon as practicable thereafter the intermediary shall -

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

(b) notify the police of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary.

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

a) follow the relevant procedure set out in any code of conduct that is applicable to such intermediary under section 19; or
(b) notify the police and the Minister.
(3) Upon being notified in respect of any information under subsection (2), the Minister may direct the intermediary to –
(a) remove the electronic communication from any information processing system within the control of the intermediary; and
(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication.
(4) An intermediary 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 provides services in respect of information in an electronic communication, for any action the intermediary takes in good faith in exercise of the powers conferred by, or as directed by the Minister under, this section.

Codes of conduct and standards for intermediaries and e-commerce service providers

19. (1) If a code of conduct is approved or a standard is appointed by the Minister under this section to apply to intermediaries or e-commerce service providers, those – intermediaries or e-commerce service providers shall comply with such code of conduct or standard.
(2) An intermediary or e-commerce service provider who fails to comply with an approved code of conduct or appointed standard, shall in the first instance be given a written warning by the Minister and the Minister may direct that person to cease and desist or otherwise to correct his practices, and, if that person fails to do so within such period as may be specified in the direction, he commits an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars and if the offence is a continuing one to a further fine of five hundred dollars for each day the offence continues.
(3) If the Minister is satisfied that a body or organization represents intermediaries or e-commerce service providers, the Minister may, by notice given to the body or organization, request the body or organization to -
(a) develop a code of conduct that applies to

intermediaries or e-commerce service providers and that deals with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and

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

(4) If the Minister is satisfied with the code of conduct provided under subsection (3), the Minister shall approve the code of conduct by notice published in the Gazette and thereupon the code of conduct will apply to intermediaries or e-commerce service providers as the case may be, as may be specified in the notice.

(5) If the Minister is satisfied that -

(a) no body or organization represents intermediaries or e-commerce service providers; or

(b) a body or organization to which notice is given under subsection (3) has not complied with the request of the Minister under that subsection, the Minister may, by notice published in the Gazette, appoint a standard that applies to intermediaries or e-commerce service providers.

(6) If the Minister has approved a code of conduct or appointed a standard that applies to intermediaries or e-commerce service providers and -

(a) the Minister receives notice from a body or organization representing intermediaries or e-commerce service providers of proposals to amend the code of conduct or standard; or

(b) the Minister no longer considers that the code of conduct or standard is appropriate,

the Minister may, by notice published in the Gazette, revoke or amend any existing code of conduct or standard.

(7) References in this section to intermediaries or e-commerce service providers include reference to a particular class of intermediary or e-commerce service provider.

PART IV
E-COMMERCE ADVISORY BOARD

E-commerce Advisory Board.

20. (1) There shall be a board to be known as the "E-Commerce Advisory Board" for the purpose

of providing advice to the Minister on matters connected with the discharge of his functions under this Act and the development of e-commerce and the information and communications technology sector generally.

(2) The Minister shall appoint the members of the Board by notice published in the Gazette.

(3) The Board shall consist of not less than five or more than nine persons appearing to the Minister to be knowledgeable about electronic commerce, information technology, communications, finance education, law or international business.

(4) The Minister shall designate one of the persons appointed a member under subsection (2) to be the chairman of the Board.

(5) The Board shall determine its own procedure.

(6) The persons appointed under subsection (2) shall hold office for such period and on such terms as may be determined by the Minister.

(7) The function of the Board is to advise the Minister on any matter referred to it by the Minister or which, of its own initiative, the Board considers appropriate.

PART V
DATA PROTECTION

Data protection

21. (1) The Minister may make regulations prescribing standards for the processing of personal data whether or not the personal data originated within Guyana.

(2) Regulations made under subsection (1) may provide for -

(a) the protection of privacy;

(b) the voluntary registration and de-registration to those standards by data controllers and data processors;

(c) the establishment of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to those standards and the dates of such registrations or de-registration and the countries in respect of which the registration or de-registration applies;

(d) the application of those standards to the countries specified in the regulations;

(e) different standards to be applied in respect of personal data originating from different countries; and

(f) such matters as may be necessary or convenient for giving effect to this Part or for its administration.

(3) A data controller or data processor who voluntarily registers to a standards prescribed in regulations made under subsection (1) and who fails to comply with that standard, as it may be amended from time to time, in respect of any personal data originating from a country to which the standard applies that is collected by the data controller during the period of registration, including any time after de-registration is guilty of an offence and is liable on summary conviction to a fine not exceeding $50,000, or to imprisonment fro 6 months, or both, and if the offence of which he is convicted is continued after conviction he commits a further offence and is liable to a fine not exceeding $5,000 for every day on which the offence is continued.

Pseudonyms

22. (1) Information security service providers may, at the request of a particular signature device holder, indicate in the relevant certificate a pseudonym instead the signature device holder’s name.

(2) Where a pseudonym is indicated in accordance with subsection (1), the information security service provider shall, where necessary for the investigation by the police of an offence involving the use of electronic signatures, or where otherwise required by law to do so, transfer to the police all personal data relating to the signature device holder that is in his possession.

(3) Where personal data is transferred pursuant to subsection (2), the information security service provider shall make a record of the transfer.

(4) The Minister may by regulations prescribe information that is to be provided in addition to the personal data that is to be transferred under subsection (2).

PART VI
ENCRYPTION

Regulations for encryption

23. (1) The Minister may make regulations -

(a) respecting the use, import and export of encryption programmes or other encryption products;
(b) prohibiting the export of encryption programmes or other encryption products from Guyana generally or subject to such restrictions as may be prescribed.
(2) Subject to any regulations made under subsections (1), a person may use any encryption programmes or other encryption product of any bit size or other measure of the strength of the encryption that has lawfully come into the possession of that person.

PART VII
ELECTRONIC SIGNATURES

Equal treatment of signatures

24. Except as provided in section 26, the provisions of this law shall not be applied so as to exclude, restrict, or deprive of legal effect, any method of creating an electronic signature which -
(a) satisfies the requirements of section 26(1); or
(b) otherwise meets the requirements of an applicable statutory provision, rule of law, contract or deed.

Compliance with a requirement for a signature

25. (1) Where the signature of a person is required by a statutory provision, rule of law, contract or deed, that requirement shall be met in relation to an electronic record if an electronic signature is used that is as reliable as was appropriate for the purpose for which the electronic record was generated or communicated, in all the circumstances, including any relevant agreements.
(2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the statutory provision, rule of law, contract or deed provides consequences for the absence of a signature.
(3) An electronic signature shall be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if -
(a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;

(b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;
(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) Sub-section (3) does not limit the ability of any person -
(a) to establish in any other way, for the purpose of satisfying the requiremet referred to in sub-section (1), the reliability of an electronic signature; or
(b) to adduce evidence of the non-reliability of an electronic signature.

Determination of standards

26. The Minister may make regulations prescribing methods which satisfy the requirements of Section 25.

Conduct of a person relying on an electronic signature

27. A person relying on an electronic signature shall bear the legal consequences of his failure to -

(a) take reasonable steps to verify the reliability of an electronic signature; or
(b) where an electronic signature is supported by a certificate, take reasonable steps to -
(i) verify the validity, suspension or revocation of the certificate; or
(ii) observe any limitation with respect to the certificate.

Recognition of foreign certificates and electronic signatures

28. (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, not to the jurisdiction in which the issuer had its place of business.
(2) If the Minister considers that the practices of a foreign information security service provider provide a level of reliability at least equivalent to that required of information security service providers in

order that they may be approved under section 31, he may by notice published in the Gazette recognize certificates or classes of certificates issued by the foreign provider as legally equivalent to certificates issued by information security service providers approved under section 31.

(3) The Minister may, by notice published in the Gazette, recognize signatures complying with the laws of a foreign jurisdiction relating to electronic signatures as legally equivalent to signatures issued by information security service providers approved under section 31 if the laws of the other foreign jurisdiction require a level of reliability at least equivalent to that required for such signatures under this Law.

(4) The Minster may make regulations prescribing the matters to be taken into account by the Minister when deciding whether to exercise his powers under subsections (2) and (3).

(5) Notwithstanding subsections (2) and (3), parties to commercial and other transactions may specify that a particular information security service provider, class of information security service providers or class of certificates shall be used in connection with messages or signatures submitted to them.

(6) Where, not withstanding subsections (2) and (3), the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognized as sufficient for the purpose of cross-border recognition in respect of that transaction.

Notarization and acknowledgement

29. Where information or a signature, document or record is required by a statutory provision or rule of law, or by contract or deed to be notarized, 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.

PART VIII
INFORMATION SECURITY SERVICE PROVIDERS

Register of approved providers

30. (1) The Minister may establish and maintain a register of approved information security services, and of providers of such services, which shall contain particulars of every person who, or service which, is for the time being approved under any arrangements in force under section 31.

(2) The Minister may make regulations prescribing the particulars that are to be included in entries in the register maintained under subsection (1).

(3) The Minister shall -

(a) allow public inspection at all times of an electronic copy of the register; and

(b) publicise any withdrawal or modification of an approval under section 31,

in accordance with arrangements prescribed by the Minster in regulations.

Arrangements for the grant of approvals

31. The Minster may make regulations enabling the Minister to grant approvals, whether subject to conditions or otherwise, on payment of a prescribed fee, to persons who -

(a) are providing information security services in Guyana, or are proposing to do so; and

(b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in Guyana or elsewhere.

Revocation of approvals

32. (1) Subject to subsection (2) the Minister, if satisfied that an approved information security service provider no longer meets the relevant criteria as specified in the regulations referred to in section 31, may, by notice in the Gazette, revoke an approval given under that section.

(2) Before revoking an approval under subsection (1), the Minister shall give notice in writing to the authorised information security service provider of his intention to do so and indicating his reasons for the proposed revocation, and shall invite the service provider, within 14 days of notice, to submit representations in writing as to why the authorization should not be revoked, and the Minister shall consider those

representations.

Provision of information security services.

33. (1) References in this Part to the provision of an information security service do not include references to the supply of, or of any right to use, computer software or computer hardware unless the supply or the right to use is integral to the provision of information security services which do not consist of such a supply or right to use.

(2) For the purpose of the Part information security service providers are provided in Guyana if they are provided from premises in Guyana and -

(a) they are provided to a person who is in Guyana when he makes use of the services; or

(b) they are provided to a person who makes use of the services for the purposes of a business carried on in Guyana or from premises in Guyana.

Conduct of the information security service provider.

34. (1) An information security service provider shall-

(a) act in accordance with the representation it makes with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representation made by it -

(i) that are relevant to the certificate throughout its life cycle; or

(ii) which are included in the certificate

(c) provide reasonably accessible means which enable a person who relies on the certificate to ascertain from the certificate -

(i) the identity of the information security service provider;

(ii) that the person who is identified in the certificate had control of the signature device at the time of signing;

(iii) that the signature device was operational on or before the date when the certificate was issued;

(d) provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise -

(i) the method used to identify the signature device holder;

(ii) any limitation on the purpose or value for

which the signature device of the certificate may be used;
(iii) that the signature device is operational and has not been compromised;
(iv) any limitation on the scope or extent of liability stipulated by the information security service provider;
(v) whether means exist for the signature device holder to give notice that a signature device has been compromised; and
(vi) whether a timely revocation service is offered;
(e) provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and
(f) utilize trustworthy systems, procedures, and human resources in performing its services.
(2) An information security service provider shall be liable for its failure to satisfy the requirements of subsection (1)

Criteria for determining trustworthiness.

35. The Minster may make regulations prescribing the factors to which regard shall be had in determine whether, and the extent to which, systems, procedures, and human resources are trustworthy for the purposes of section 35(1)(f).

Contents of a certificate.

36. The Minster may make regulations prescribing the matters that shall be specified in a certificate.

Conduct of the signature device holder.

37. A signature device holder shall-

(a) exercise reasonable care to avoid unauthorized use of its signature device;
(b) without under delay, notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature if -
(i) the signature device holder knows that the signature device has been compromised; or
(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised; and
(c) where a certificate is used to support the electronic signature, exercise reasonable

care to ensure that the accuracy and completeness of all material representation made by the signature device holder, which are relevant to the certificate throughout its lifecycle, or which are to be included in the certificate.

PART IX
GENERAL

General provisions as to prosecutions under the Act.

38. (1) Where a body corporate commits an offence under this Act or regulations made hereunder, every person who at the time of the commission of the offence was a director, officer, general manager, chief executive officer, managing director of the corporation, or a person purporting to act in any such capacity commits the like offence unless he proves that the contravention took place without his consent or that he exercised all due diligence to prevent the commission of the offence.

(2) Unless otherwise expressly provided for under this Act and regulations made pursuant thereto, the penalty for conviction of an offence under this Act shall be -

(a) on summary conviction, to a fine not exceeding three thousand dollars or to imprisonment for twelve months, or to both;

(b) on conviction on information, to a fine not exceeding one hundred thousand dollars or to imprisonment for ten years, or to both.

Regulations.

39. (1) The governing authority may make regulations -

(c) for the purpose of authorising, prohibiting or regulating the use of the .gy domain name or any successor domain name for Guyana;

(d) prescribing for the purposes of the registration of the .gy domain name or any successor domain name for Guyana-

(i) designated registration authorities,

(ii) the form of registration,

(iii) the period when registration stays in force,

(iv) the manner, the terms and the period for renewal of registration,

(v) the circumstances and manner in which registration may be granted, renewed or refused by the registration authorities,

(vi) the appeal process,

(vii) the fees to be paid on the grant or renewal of registration and the time and manner they are to be paid; and
(viii) such other matters relating to the registration of domain names;
(c) generally for the better carrying out of the provisions of this Act.