BILL

To provide for a general framework for the promotion of the use of electronic transactions in government services and private contracts; to provide for the legal recognition of electronic transactions; to provide for the admission of electronic evidence; to provide for consumer protection in electronic commerce; to regulate the liability of service providers for actions of their clients; to provide for the protection of critical and important data; to create certain offences; to create certain powers for the investigation of offences and to provide for matters incidental thereto.

(Introduced by the Minister of Information Communications and technology)

ARRANGEMENT OF SECTIONS

Section

BE IT ENACTED, as passed by the Parliament, and assented to by the President, of the Republic of Namibia, as follows:

CHAPTER 1
PRELIMINARY PROVISIONS

Definitions

1. In this Act, unless the context indicates otherwise –

"accredit" means accredit under Chapter 5;

"addressee" of a data message, means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary in respect of that data message;

"advanced electronic signature" means an electronic signature which is designed so that together with a security procedure it is possible to verify that the signature –

(a) is unique to the signer for the purpose for which it is used;

(b) can be used to identify objectively the signer of the data message;

(c) was created and affixed to the data message by the signer or using a means under the sole control of the signer; or

(d) was created and is linked to the data message to which it relates in a manner such that any changes in the data message can be detected;

"Authority" means the Communications Regulatory Authority of Namibia established by

section 4 of the Communications Act, 2009 (Act No. 8 of 2009);

"automated message system" means a pre-programmed system or other electronic or other automated means, including a computer program, used to initiate an action, respond to data messages or generate other performances in whole or in part, without review or intervention by a human being each time an action is initiated or a response is generated by the system;

"communications" means electronic communications;

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

"computer evidence" means data evidence or information evidence;

"Council" means the Electronic Information Systems Management Advisory Council established by section 4;

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

"data evidence" means evidence of any matter relevant in legal proceedings if that matter is represented in a computer system directly and can be made readily understandable to a human being without requiring any special skills or knowledge on the part of any person and includes a display, print out or other output of that data;

"data message" means data generated, displayed, sent, received or stored by electronic or similar means and which appears to a user as a logical unit, including, but not limited to, electronic data interchange (EDI), electronic mail, a web page, mobile communications, such as SMS messages, audio and video recordings, telegram, telex or telecopy;

"digital certificate" means data or a device which enables a person to verify that a data message has been sent or created by a specific person and which data or device has been issued by a third party or by an information system on behalf of that third party;

"electronic" means represented by an electric potential difference, the flow of current, any other state of an electronic component, the state of a mechanical component, the state of magnetisation of any matter or by any other means whereby information can be represented in matter or radiation and can be processed by a computer system or an information system;

"electronic signature" means data including a sound, symbol or process, executed or adopted to identify a person and to indicate that person's approval or intention in respect of the information contained in a data message and which is attached to or logically associated with such data message;

"excluded laws"means –

(a) the Wills Act, 1953 (Act No. 7 of 1953);

(b) the Alienation of Land Act, 1981 (Act No. 68 of 1981);

(c) the Stamp Duties Act, 1993(Act No. 15 of 1993);

(d) the Bills of Exchange Act,2003 (Act No 22 of 2003); and

(e) any law which requires that a person that borrows money or to whom credit is provided, must conclude a written contract or must sign such contract or another document;

"information evidence" means evidence of a matter relevant in legal proceedings that is not stored in a computer system, but can be produced from data stored in a computer system by means of a statistical, mathematical or logical process;

"information system" means facilities for generating, sending, receiving, storing or processing data or data messages and includes a device or combination of devices, including input and output devices, capable of being used in conjunction with external files, which contain computer systems, computer programs, electronic instructions, input and output data, that performs logic, arithmetic, data storage, retrieval, communication, control or other functions;

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

"Minister" means the Minister responsible for technology;

"Ministry" means the Ministry responsible for technology;

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

"Permanent Secretary" means the permanent secretary of the Ministry;

"prescribe" means prescribe by regulation;

"secure electronic signature" means an advanced electronic signature complying with the requirements prescribed under section 20(3) for a secure electronic signature;

"security procedure" means a process involving one or more of the purposes referred to in section 41(1);

"security product" means a product that as part of its functionality has one or more of the purposes referred to in section 41(1);

"security service" means a service (including the issuing of digital certificates) which involves anything with a purpose referred to in section 41(1);

"this Act" includes regulations made in terms of this Act;

"transaction" means an action or set of actions of either a commercial or non-commercial nature, including the provision of information and e-government services.

"web page" means a data message providing for an information browsing framework that allows a user to locate and access information stored on an information system and to follow references to other information, facilities or functions.

Objects of Act

2. The objects of this Act are –

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

(b) to remove and prevent barriers to electronic transactions and related communications;

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

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

(e) to develop a safe, secure and effective environment for the consumer, business and public agencies or bodies to conduct and use electronic transactions;

(f) to promote the development of electronic transaction services responsive to the needs of online 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 communications; and

(i) to ensure that the interest and image of Namibia are not compromised through the use of electronic transactions and communications.

General functions and powers of Minister

3. The Minister must after consultation with the Council –

(a) make all necessary regulations, for the development, management, and facilitation of electronic transactions and related communications use in Namibia;

(b) co-ordinate information technology developments at national level; and

(c) monitor and ensure compliance with this Act and such other policy documents relating to the objects of this Act which have been adopted by the Namibian Government.

CHAPTER 2
ELECTRONIC INFORMATION SYSTEMS MANAGEMENT ADVISORY COUNCIL

Establishment of Council

4. There is established a body, to be known as the Electronic Information Systems Management Advisory Council, which may be referred to by the abbreviation "EISMAC", to exercise the powers and perform the functions conferred on and assigned to it by or under this Act.

Composition of Council

5. (1) The Council consists of five members appointed by the Minister.

(2) The members of the Council must have relevant knowledge relating to the matters regulated by this Act or in general the use of computer systems, information technology, data processing and electronic communications systems.

(3) The Minister must appoint one member of the Council as Chairperson and the Council must elect another of its members as the Vice-Chairperson.

Disqualification

6. A person is not eligible to be appointed as a member of the Council, if he or she –

(a) is not a Namibian citizen or lawfully admitted to Namibia for permanent residence, or does not reside in Namibia;

(b) is a member of the National Assembly of Namibia or a regional council established under section 2 of the Regional Councils Act, 1992 (Act No. 2 of 1992);

(c) is an unrehabilitated insolvent;

(d) is of unsound mind; or

(e) has within ten years from the date of appointment been convicted of an offence involving an element of dishonesty, or of a contravention of this Act, or of any other law relating to the usage of information and communications technologies or systems.

Term of office

7. (1) Subject to section 8, a member holds office for a period of three years.

(2) A member whose term of office has expired is eligible for reappointment.

Vacating of office and filling of vacancy

8. (1) A member ceases to hold office if he or she –

(a) becomes subject to a disqualification referred to in section 6;

(b) resigns by giving notice in writing addressed to the Minister ;

(c) is removed from office under subsection (2).

(2) The Minister may remove a member from office by notice in writing, if –

(a) there is good reason for doing so; and

(b) the member has been given reasonable opportunity of making representations to the Minister.

(3) If the office of a member becomes vacant before the expiration of his or her term of office, the Minister must appoint, another person to fill the vacancy for the unexpired portion of that term.

Remuneration

9. A member or a member of a committee, who is not in the full time employment of the State, must be paid such remuneration and allowances as the Minister, with the concurrence of the Minister responsible for finance, may determine.

Meetings of Council

10. (1) The first meeting of the Council must be held at a time and place as determined by the Minister, and thereafter the Council must meet at the times and places determined by the Council.

(2) The Chairperson must convene the next meeting if for any reason a meeting cannot take place at the date and time determined by the Council.

(3) The Council must meet at least four times a year.

(4) The Chairperson may at any time, and must upon receipt of a request in writing of at least three other members or of the Minister, convene a special meeting of the Council.

(5) The Chairperson or, in the absence of the Chairperson, the Vice-Chairperson must preside at a meeting of the Council and, if neither of them is present, the members present must elect a member to preside at that meeting.

(6) At a meeting of the Council –

(a) a quorum at a meeting of the Council is three members;

(b) all questions are decided by a majority of votes of the members present and voting; and

(c) the member presiding has a deliberative vote and, in the event of an equality of votes, also a casting vote.

(7) The Council must, on a request in writing of the Minister, consider any matter specified by the Minister in relation to the Council's functions.

(8) Unless the Council determines otherwise, the Permanent Secretary, or his or her delegate, must attend the meetings of the Council and may take part in deliberations, but has no vote.

(9) The Council may permit any person who has expert knowledge of a matter which is before the Council or a committee for determination to attend a meeting of the Council or the committee and take part in deliberations in relation to that matter, but that person has no vote.

(10) Subject to this Act, the Council –

(a) may regulate its own proceedings;

(b) must cause minutes of proceedings and decisions at each meeting of the Council to be kept; and

(c) must submit a copy of the minutes to the Minister as soon as possible after the minutes have been approved by the Council.

Committees

11. (1) The Council may establish such committees as it deems convenient with the approval of the Minister –

(a) to advise the Council on any matter in relation to the Council's functions; or

(b) to perform, subject to the directions of the Council, any function of the Council which the Council delegates to it in writing.

(2) The Council must establish a consumer affairs committee which must consist of three members of whom at least one must be a member of the Council.

(3) A committee may consist of one or more members of the Council or of one or more members of the Council and such other persons whom the Council considers to be suitable.

(4) The Council must appoint a member of the Council as chairperson of a committee.

(5) The Council may at any time dissolve or reconstitute a committee.

Disclosure of interest

12. (1) If a member of the Council or of a committee has a direct or indirect financial or other interest in any matter which is the subject of consideration by the Council or the

committee and which may cause a conflict of interest in the proper performance of his or her duties as such a member, he or she must disclose that interest to the Council or to the committee as soon as is practicable after the relevant facts have come to his or her knowledge.

(2) A person who has an interest referred to in subsection (1) –

(a) if he or she is present at a meeting of the Council or the committee at which the matter is to be considered, must disclose the nature of his or her interest to the meeting immediately before the matter is considered; or

(b) if he or she is aware that the matter is to be considered at a meeting of the Council or the committee at which he or she does not intend to be present, must disclose the nature of his or her interest to the chairperson of the Council or the committee before the meeting is held.

(3) A member of the Council or of a committee who has an interest referred to in subsection (1) may not –

(a) be present during any deliberation; and

(b) take part in any decision of the Council or the committee in relation to the matter in question.

(4) A disclosure by a member under this section must be recorded in the minutes of the relevant meeting of the Council or committee.

(5) A member of the Council or a committee may not –

(a) use any confidential information obtained in the performance of his or her functions as a member to obtain, directly or indirectly, a financial or other advantage for himself or herself or any other person;

(b) disclose any confidential information obtained in the performance of his or her

functions as a member unless such disclosure is required by the provisions of another law or by an order of court.

(6) A person who contravenes or fails to comply with any provision of this section, commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

Functions of Council

13. The functions of the Council are to –

(a) advise the Minister on appropriate amendments of this Act;

(b) advise the Minister on the making of or the amendment of regulations under this Act;

(c) render the necessary assistance to the Minister with the monitoring of compliance with policy documents referred to in section 3(c);

(d) recommend to any functionary the taking of any action by that functionary in order to promote the objects of this Act or in order to comply with policy documents referred to in section 3(c);

(e) recommend to the Minister the issuing of guidelines under section 14.

Guidelines

14. (1) The Minister may on the recommendation of the Council by notice in the *Gazette* issue guidelines on any matter relating to the operation, design and administration of information or communications systems.

(2) Guidelines referred to in subsection (1), may relate to –

(a) compliance with any standard or specification;

(b) interoperability with any specified system;

(c) the handling or creation of any specified data format or the ability to handle any specified communications protocol.

(3) Guidelines referred to in subsection (1) may specify any matter with reference to any published standards document, whether by a standards body created by or under the laws of any country, an international standards body, any group created by any industry or any document issued by the producer of any hardware or software: Provided that the guidelines in question must specify a place where such standard document may be inspected during such hours and at such places as may be specified.

(4) If it is necessary to exercise any power, or to accept a tender, conclude a contract or to perform any similar action, non-compliance with the guidelines issued in terms of this section is a ground for refusal to perform such action, if a matter contained in a guideline is relevant for the performance of the action in question.

Secretariat

15. (1) The Permanent Secretary must ensure the allocation of staff members for the purpose of performing the functions, inclusive of the secretarial services, of the Council, with due regard to the resources of the Ministry.

(2) The Council may with the approval of the Minister appoint a consultant to perform any service to the Council or a committee that may be necessary or desirable for the performance of its functions.

CHAPTER 3
LEGAL RECOGNITION AND EFFECT OF DATA MESSAGES AND ELECTRONIC TRANSACTIONS

Application of this Chapter

16. (1) In this Chapter any reference to a law is construed to refer to a law applicable in Namibia whether it has been enacted before or after the commencement of this Act and also to this Act.

(2) Subsection (1) is not construed in such a manner that it –

(a) invalidates any transaction or act performed before the commencement of this Act;

(b) that it will create criminal or civil liability for any act performed before the commencement of this Act.

(3) Except for section 18 and 25 –

(a) no provision of this Chapter relates to any matter regulated in the excluded laws; and

(b) no reference in this Chapter to "law" relates to any provision of the excluded laws.

Legal recognition of data messages

17. (1) No statement, representation, expression of will or intention, transaction or communication is without legal effect, validity or enforceability solely on the ground that it is in the form of a data message.

(2) Despite subsection (1), persons may by agreement regulate the effect, use and requirements for data messages as it relates to dealings among themselves.

(3) Subject to this Act, any other law or any agreement, no public body may compel any person to interact with it by means of a data message.

Interpretation of power to make regulations

18. (1) Any provision in any law, whether enacted before or after the commencement of this Act, that confers a power to prescribe or determine –

(a) any form to be used for any purpose;

(b) the manner or procedure of making an application or providing any information to an institution or body,

is, unless a contrary intention appears, construed to authorise the functionary concerned to –

(i) prescribe or determine a procedure involving the use of a data message or the interaction with an automatic data entry system;

(ii) require the provision of data in any prescribed or determined computer readable format;

(iii) prescribe or determine compliance with any specified protocol or procedure;

(iv) prescribe or determine any technical or other requirement that may be necessary in order to allow or facilitate the use of information systems;

(v) prescribe or determine that a specified type of electronic signature is required;

(vi) prescribe or determine the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;

(vii) prescribe or determine that a specific class of accredited security product, service, provider of a security product or renderer of a security service must be used;

(viii) subject to any law regulating electronic payments in Namibia, prescribe or

determine the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(ix) prescribe or determine any other matter that is necessary or expedient to prescribe or determine with relation to the use of data messages or information systems.

(2) A provision in any law requiring or permitting any functionary to prescribe or determine that any information must be posted, displayed, sent or transmitted in a manner prescribed or determined by that functionary is construed to include the power to prescribe or determine a method involving the transmission of a data message or the making available of that information by means of any information system.

(3) A power to prescribe or determine a duty to store or retain information in a manner so prescribed or determined is construed to include the power to prescribe or determine a manner of storage or retention that includes the storage or retention of the information in an electronic form.

(4) The powers referred to in subsection (1), (2) and (3) include the power to specify any requirement or matter with reference to any standard published by a standards body in Namibia or of another country, or or by any international organisation or industry body: Provided that the regulations in question must specify a place where such standard document may be inspected during such hours and at such places as may be prescribed.

Writing

19. A reference to writing in any law is construed to include a reference to a data message if the information contained therein is accessible so as to be usable for subsequent reference, unless –

(a) a different intention appears from the law in question;

(b) the law in question provides for a process that is incompatible with the use of

a data message or cannot be applied to a data message; or

(c) the purpose for requiring writing is in order to protect consumers.

Electronic signature

20. (1) A reference in any law, contract or any other legal instrument to a signature or the signing of a document is construed to include a reference to a secure electronic signature, unless –

(a) a contrary intention appears from the law or document concerned;

(b) the law in question provides for a process that is incompatible with the use of a secure electronic signature;

(c) the requirement that the document must be in writing, is not construed to include a data message as contemplated in section 19.

(2) Nothing in this section is construed as limiting the use of an electronic signature that is not a secure electronic signature if parties agree to such use or if a law provides for such use.

(3) The Minister may make regulations –

(a) prescribing the requirements for secure electronic signatures;

(b) prescribing a process for verifying that a secure electronic signature has been applied by a specific person;

(c) prescribing any requirement or process for applying a secure electronic signature to any data message and prescribing a procedure or requirement for determining whether a secure electronic signature has been applied to a spe-

cific data message and whether the data message has been altered since the secure electronic signature has been applied;

(d) prescribing the role and the duties of accredited service providers;

(e) prescribing any presumptions that will apply when a prescribed security procedure has been followed;

(f) prescribing anything that is necessary or expedient to prescribe with relation to a secure electronic signature.

(4) If any presumptions have been prescribed in terms of subsection (3)(e), those presumptions will be *prima facie* proof of the matter presumed in criminal proceedings and will be presumed unless the contrary is proved in civil proceedings.

Original information

21. (1) Unless a contrary intention appears, where a law requires information to be presented or retained in its original form, that requirement is met by a data message if –

(a) there exists a reliable assurance that the information has remained complete and unaltered from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information must be presented, that information is capable of being displayed in the form of a data message to the person to whom it must be presented.

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

(3) For the purposes of subsection (1)(a) –

(a) information is deemed to have remained complete and unaltered if it has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and

(b) the level of reliability must be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Production of document or information

22. (1) Unless a contrary intention appears, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if –

(a) considering all the relevant circumstances at the time that the data message was sent or generated, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that data message; and

(b) at the time the data message was sent or generated, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is deemed to have been maintained if the information has remained complete and unaltered except for –

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display.

Other requirements

23. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) Unless a contrary intention appears, where any law requires or permits a person to send a document or information by post or similar service, that requirement is met if an electronic form of that document or information is sent to the electronic address or designated information system provided by the addressee: Provided that this provision does not apply where the law requires that a document must be sent by registered post or must be delivered by hand or handed to a specific person.

Retention of electronic records

24. (1) Where the law requires that certain documents, records or information be retained, that requirement is met by electronic record retention, if –

(a) the electronic record contained therein is a data message;

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

(c) such electronic record is retained in a form that enables the identification of the origin and destination of an electronic record or data message and the date and time when it was first generated, sent or received and the date and time it was first retained; and

(d) it complies with any other requirement that may be prescribed.

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

(3) A person may use the services of another person in order to comply with subsection (1): Provided that the former person will be liable for the contravention of the provision in question if the latter person has failed to retain the information.

Admissibility and evidential weight of data messages and computer evidence

25. (1) In any legal proceedings, nothing in the application of the rules of evidence may be applied in such a manner that it would have the effect that computer evidence is inadmissible –

(a) on the sole ground that it is computer evidence; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) When evidence is admitted in terms of this section, the court must assess the weight to be given to that evidence.

(3) In assessing the evidential weight of computer evidence, the court must have regard to –

(a) the reliability of the manner in which the computer evidence was generated, stored or communicated;

(b) the integrity of the information system in which the computer evidence was recorded, stored and maintained;

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

(d) any other relevant factor.

(4) A data message made by or on behalf of a person in the ordinary course of

business, or a copy or printout of or an extract from such data message certified to be correct, is admissible in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, as evidence of the facts contained in such record, copy, printout or extract against any person, if –

(a) the affidavit has been made by the person who was in control of the information system at the time when the data message has been created;

(b) the facts stated in the affidavit justify a finding on the reliability of the manner in which the data message has been generated, stored or communicated;

(c) the facts stated in the affidavit justify a conclusion on the reliability of the manner in which the integrity of the data message was maintained; and

(d) the facts stated in the affidavit justify a conclusion on the manner in which the originator of the data message has been identified if the identity of the originator is relevant to a matter in dispute.

(5) In legal proceedings all rules of evidence must be applied in such a manner that a data message tendered as contemplated in this section is admissible if documentary evidence that is similar in all material respects would have been admissible.

(6) Any document containing data evidence and purporting to be a printout of data or information stored or created by a computer system is admissible in legal proceedings if it has been authenticated by means of admissible evidence.

(7) Evidence referred to in subsection (6) is not admissible to the extent that the evidence in the document in question is hearsay evidence, except where any rule of evidence would have rendered similar evidence admissible if the evidence in question were contained in a document.

(8) If in its opinion it is in the interest of the administration of justice, a court may

allow a person to perform a demonstration on a computer system instead of a printout if such demonstration has been performed by a person who has authenticated such demonstration by means of admissible evidence.

(9) Evidence authenticating a printout or a demonstration must be evidence of –

(a) the steps that have been taken to create the printout;

(b) the software that has been used to create the printout or demonstration;

(c) if the steps referred to in paragraph (a), require any special expertise, the nature of the qualifications or experience of the person who performed those steps;

(d) particulars of any alterations made in order to create such printout or demonstration and if no such alteration has been made, a statement to that effect; and

(e) any other fact that is relevant in order to demonstrate that the evidence is reliable and is what it purports to be.

(10) If any matter referred to in subsection (9) is not admitted by all parties in the proceedings in question, the party or person tendering the evidence in question, bears the burden of proof of all the facts referred to in that subsection.

(11) It is presumed, unless admissible evidence to the contrary is provided, that software operates correctly.

(12) No expert evidence is required to prove the operation or functionality of software that is commonly used on personal computers or other computational devices that are commonly used by persons that are not experts in the field of computer science or a related field.

(13) Information evidence is admissible in legal proceedings if such evidence is contained in an affidavit that –

(a) states the experience and qualifications of the person making that affidavit;

(b) explains the nature of the processes performed to obtain the information in question and the reason why such process is relevant for the information contained in the evidence in question; and

(c) states all the relevant conclusions embodied in that information.

(14) Information admitted in terms of subsection (13) is *prima facie* evidence of all the relevant information contained in the affidavit in question if in the opinion of the court the person making the declarations has sufficient expertise to perform the process in question and draw the conclusions in question and there is no other reason why the conclusions should not have been drawn.

(15) Information evidence may also be given by means of oral evidence or by means of a demonstration, if admissible evidence of the facts referred to in subsection (13) has also been given.

(16) No provision of this section is construed in such a manner that it would render evidence inadmissible that would have been admissible if this section has not been enacted.

Formation and validity of contracts

26. (1)Where data messages are used in the formation of a contract, that contract is not without legal effect, validity or enforceability on the sole ground that a data message has been used to make an offer or to accept an offer for that purpose.

(2) A proposal to conclude a contract made through one or more data messages, which is not addressed to one or more specific person but is generally accessible to the public or a specific portion of the public (including proposals that make use of interactive

applications for the placement of orders through such information systems) is presumed to be an invitation to make offers, unless it clearly indicates the intention of the person making the proposal to be bound in case of acceptance.

(3) This section does not confer any validity to transactions referred to in the excluded laws.

Incorporation by reference

27. (1) Subject to subsection (2), information may not be denied legal effect, validity or enforceability solely on the ground that it is not contained in the data message purporting to give rise to such legal effect, validity or enforceability, if such information is referred to in that data message in a manner that indicates that that information is regarded to have been incorporated in that data message.

(2) The onus to prove that information referred to as contemplated in subsection (1) is on the party who originated that data message and such onus is only discharged if –

(a) it is proved that the data message clearly referred to the incorporated information as contemplated in subsection (1);

(b) it was possible for a person who read the referring data message to easily read the incorporated information;

(c) the information claimed to be incorporated was actually the information referred to by the incorporating message at the time when the referring message was accessed.

Variation by agreement

28. The provisions of this Chapter apply, unless the parties involved in generating, sending, receiving, storing or otherwise processing data messages, have agreed otherwise.

Time of dispatch and receipt of data messages

29. (1) Subject to subsection (2), for all purposes in law it is deemed that a data message has been dispatched at the time when it enters an information system outside the control of the originator or of the person that sent the data message on behalf of the originator.

(2) If the originator and the addressee are in the same information system, it is deemed for all purposes in law that the data message has been dispatched at the time when it is capable of being retrieved by the addressee.

(3) For all purposes in law, a data message sent to an electronic address designated by the addressee is deemed to have been received at the time when it becomes capable of being retrieved by the addressee at that electronic address.

(4) For all purposes in law, a data message sent to an electronic address different from the electronic address referred to in subsection (3) is deemed to have been received at that address at the time when it becomes capable of being retrieved by the addressee at that address and the addressee has become aware that the electronic communication has been sent to that address.

Place of dispatch and receipt of data messages

30. (1) For all purposes in law it is deemed that a data message have been dispatched at the place of business of the originator, and is deemed to have been received at the place of business of the addressee.

(2) For the purposes of this section a place of business is any place where a person maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.

(3) If a person has more than one place of business, the place of business contemplated in subsection (2) is –

(a) the place of business which has the closest relationship to the underlying transaction having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract; or

(b) where there is no underlying transaction, the principal place of business.

(4) If the originator or the addressee does not have a place of business, it is deemed for the purposes of this section that that person has a place of business at that persons habitual residence.

Time and place of contract formation

31. (1) If parties conclude a contract by means of data messages such contract is formed at the time when and the place where the acceptance of the offer becomes effective as provided by subsection (3).

(2) An offer in the form of a data message becomes effective –

(a) at the time when it is deemed to have been received by the offeree as provided by section 29(3) or 29(4) as the case may be; and

(b) at the place where it is deemed to have been received by the offeree as provided by section 30.

(3) The acceptance of an offer in the form of a data message becomes effective –

(a) at the time when it is deemed to have been received by the offerer as provided by section 29(3) or (4), as the case may be; and

(b) at the place where it is deemed to have been received by the offerer as provided by section 30.

Attribution of data messages

32. For all purposes in law, it is deemed that a person has sent a data message, if –

(a) that person has sent the message personally;

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

(c) the message has been sent by an information system programmed by or on behalf of the originator to operate automatically unless the originator proves that the information system did not properly execute such programming.

Automated message systems

33. (1) A contract formed by the interaction of an automated message system and a person, or by the interaction of automated message systems, are not without legal effect, validity or enforceability on the sole ground that no natural person reviewed any of the individual actions carried out by the systems or the resulting contract.

(2) Where a natural person makes an input error in a data message 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 data message in which the input error was made if –

(a) the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the data message and wishes to cancel the contract or correct the input error;

(b) the person, or the party on whose behalf that person was acting, takes reasonable steps, including steps that conform to the instructions given by the other party, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services, or to correct the

input error; and

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

(3) If a person who has made an input error as contemplated in subsection (2), has paid for any goods or services prior to exercising a right referred to in that subsection, such person is entitled to a full refund of such payment, which refund must be made within 30 days of the date of cancellation.

(4) Nothing in this section affects the application of any rule of law that may govern the consequences of any errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in subsection (1).

CHAPTER 4
CONSUMER PROTECTION

Information to be provided

34. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered or if it is not offered on a website in the data message in which it is offered –

(a) its full contact details, including its place of business, e-mail addresses and telefax number;

(b) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

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

other fees or costs;

(d) any terms of agreement and the manner and period within which consumers can access and maintain a full record of the transaction; and

(e) the rights conferred to consumers by section 35, where applicable.

(2) The supplier must provide a consumer with an opportunity –

(a) to review the entire electronic transaction;

(b) to correct any mistakes; and

(c) to withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3) –

(a) the consumer must return the performance of the supplier or, where applicable, cease using the services performed;

(b) the supplier must refund all payments made by the consumer minus the direct cost of returning the goods.

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

(6) The supplier is liable for any damage suffered by a consumer due to a failure by

the supplier to comply with subsection (5).

Cooling-off period

35. (1) Subject to subsection (5), a consumer is entitled to cancel without reason and without penalty any transaction for the supply –

(a) of goods within seven days after the date of the receipt of the goods; or

(b) of services within seven days after the date of the conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund must be made within 30 days of the date of cancellation.

(4) This section is not construed as prejudicing the rights of a consumer provided for in any other law.

(5) This section does not apply to an electronic transaction –

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

(b) to goods and services sold by way of an auction;

(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(d) for services which began with the consumer's consent before the end of the seven-day period referred to in subsection (1)(b);

(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(f) where the goods-

(i) are made to the consumer's specifications;

(ii) are clearly personalised;

(iii) by reason of their nature cannot be returned; or

(iv) are likely to deteriorate or expire rapidly;

(g) where audio or video recordings or computer software was unsealed by the consumer;

(h) for the sale of newspapers, periodicals, magazines or books;

(i) for the provision of gaming, online gambling and lottery services insofar as such services are legally provided in Namibia; and

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

Unsolicited goods, services or communications

36. (1) Marketing (to a consumer or any other person) by means of data message must include the following information in all such data messages –

(a) the originator's identity and contact details including its place of business, e-mail, addresses and telefax number;

(b) a valid and operational opt-out facility from receiving similar communications in future; and

(c) the identifying particulars of the source from which the originator obtained the addressee's personal information.

(2) Unsolicited commercial messages may only be sent to addressees where the opt-in requirement is met.

(3) The opt-in requirement is met if –

(a) the addressee's e-mail address and other personal information was collected by the originator of the message in the course of a sale or negotiations for a sale;

b) the originator only sends promotional messages relating to its similar products and services to the addressee;

(c) when the personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out (free of charge except for the cost of transmission) and the addressee declined to opt-out; and

(d) the opportunity to opt-out is provided by the originator to the addressee with every subsequent message.

(4) In spite of any wording in the message concerned, no contract is formed where the addressee has failed to respond to an unsolicited communication.

(5) An originator who fails to provide the recipient with an operational opt-out facility referred to in subsections (1)(b) and 3(d) commits an offence.

(6) Any originator who persists in intentionally sending unsolicited commercial communications to an addressee, who has advised the originator by means of the opt-out facility that such communications are unwelcome, commits an offence.

(7) Any person whose goods or services are advertised in contravention of this section commits an offence.

(8) A person who commits an offence as contemplated in subsection (5), (6) or (7) is on conviction liable to a fine not exceeding N$500 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

Performance

37. (1) The supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise

(2) Where a supplier has failed to execute the order within 30 days or within the agreed period the consumer may cancel the agreement with seven days written notice.

(3) If a supplier is unable to perform in terms of the contract on the grounds that the goods or services ordered are unavailable, the supplier must immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

Applicability of foreign law

38. The protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the contract in question.

Non-exclusion

39. Any provision in a contract which excludes any rights provided for in this Chapter is null and void.

Complaints to Online Consumer Affairs Committee

40. (1) A consumer may lodge a complaint with the Online Consumer Affairs Committee in respect of any non-compliance with the provisions of this Chapter by a supplier.

(2) After the committee has investigated the matter, it may after giving the supplier an opportunity to be heard –

(a) order the supplier to comply with the provision of this Act which has been contravened; or

(b) impose a fine not exceeding N$20 000 which fine may be collected as a debt due to the state.

(3) A supplier who fails to comply with an order made in terms of subsection (2)(a) commits an offence and is on conviction liable to a fine not exceeding N$50 000 or imprisonment for a period not exceeding one year or to both such fine and such imprisonment.

CHAPTER 5
ACCREDITATION OF SECURITY SERVICES OR PRODUCTS

Security products or services

41. (1) A product or service may be accredited by the Authority to comply with the requirements of one or more classes prescribed under subsection (2) if such product or service –

(a) has as its purpose the encryption or decryption of data;

(b) ensures that data has not been altered;

(c) ensures that data has been altered or created by a specific person only;

(d) creates keys for the encryption or decryption of data;

(e) prevents unauthorised persons from accessing an information system or certain functions of an information system;

(f) enables the detection of unauthorised access or tampering with data or an information system;

(g) has for its purpose the linking of a specific person with a transaction or action;

(h) has any other purpose relating to the security or integrity of data or an information system, or the linking of any action to a specific information system or person; or

(i) has a combination of such purposes.

(2) The Minister may prescribe different classes of security services, products, providers of security products or renderers of security services which classes may include one or more classes of issuers of digital certificates.

Accreditation

42. (1) A person who supplies a security product or who renders a security service, may apply in the prescribed manner to the Authority for the accreditation of that product or service or may apply to the Authority to be accredited as a supplier of that security product or as a provider of that security service.

(2) The Authority may on the application of any person or on its own motion accredit a product available in Namibia, or a service that is provided by a person outside Namibia in a class prescribed in section 41(2).

(3) The Authority may accredit a person in a class prescribed under section 41(2) as the provider of a specific security product or as the renderer of a specific security service if it is of the opinion that –

(a) the product or service is sufficiently secure for the purpose concerned; and

(b) the person who provides the product or who renders the service has the necessary expertise to ensure that the product or service as the case may be, is provided or rendered in such a manner that the process concerned is as secure as is required for the purpose concerned.

(4) The Authority must issue a certificate of accreditation in respect of every product, service, provider or renderer accredited in terms of subsection (3) which must state –

(a) the name and address of the person to whom the certificate has been issued;

(b) the name and any information necessary to identify the product or service for which the certificate has been issued;

(c) the purpose for which the product or service has been accredited;

(d) the class in which the service or product has been accredited; and

(e) any other relevant information that the Authority considers necessary.

(5) The Authority must make an accreditation in terms of this section known in the prescribed manner.

(6) Different methods may be prescribed in terms of subsection (5) in respect of different types of accreditation.

Powers and duties of Authority in relation to accreditation

43. (1) The Authority has all the powers with relation to a person whose service or product has been accredited that it has in terms of the Communications Act, 2009 (Act No. 8 of 2009) with relation to the provider of telecommunications services contemplated in that Act and –

(a) may enforce any provision of this Act as if it were a provision of that Act; and

(b) enforce any condition imposed when a product or service has been accredited as if that condition were a licence condition imposed in terms of that Act.

(2) The Authority may without giving notice perform a security test or cause such test to be performed by a person that in its view has sufficient skill, in respect of the information system of a person whose product or service has been accredited.

(3) A security test referred to in subsection (2) may involve the access of the system without authorisation as contemplated in Chapter 8 which access is lawful and is not a contravention of section 63.

(4) The Authority must in the prescribed manner maintain a publicly accessible database in respect of –

(a) all security products and services accredited;

(b) all accredited providers of security products and all accredited renderers of security services;

(c) revoked and suspended accreditations; and

(d) such other information as may be prescribed.

Criteria for accreditation

44. The Authority may not accredit security services, products, providers of security products or renderers of security services, unless the product, service, provider and renderer comply with the requirements prescribed for the class of service or product in question.

Conditions for accreditation

45. (1) The Authority may impose any conditions in respect of an accreditation in terms of this Chapter.

(2) Conditions imposed in terms of subsection (1) may relate to –

(a) the financial well-being of the provider of the service or product;

(b) the technical competence of the provider of the service or product and its employees or partners;

(c) the reporting of any matter to the Authority, the keeping of records and the provision of any information to the Authority on request;

(d) the making available of information to the public or to its clients, or to persons requesting verification or authentication from the provider;

(e) the circumstances under which digital certificates, keys or other authentication data must be revoked or changed, as well as any procedural matter or any other duty relating to such change or revocation;

(f) the steps which must be taken and the duties or other requirements to which an accredited service provider is subject if a security breach occurs;

(g) the procedure and duties to be imposed upon the provider of the product or service if it seizes its operation and may include the payment of a deposit or the provision of other security for the performance of such actions, in order to ensure that the service is seized with the minimum possible disruption; and

(h) any other matter that may be necessary or expedient in order to ensure that a secure and efficient authentication service is rendered to the Namibian public and that the service or product is in accordance with internationally accepted technical standards.

Revocation or suspension of accreditation

46. (1) The Authority may suspend or revoke an accreditation if it is satisfied that the product, service, provider or renderer has failed to comply with, or fails to meet any of the requirements, conditions or restrictions subject to which accreditation was granted.

(2) Subject to subsection (3), the Authority may not suspend or revoke an accreditation in terms of subsection (1) unless –

(a) it has notified the provider of the service or product in question in writing of its intention to do so;

(b) it has given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted; and

(c) it has given the provider in question the opportunity to respond to the allegations in writing; and remedy the alleged failure within a reasonable time if in its opinion such remedy is possible.

(3) The Authority may suspend any accreditation with immediate effect for a period not exceeding 90 days, pending implementation of the procedures necessary to remedy a failure referred to in subsection (1), if the continued accreditation is reasonably likely to result in irreparable harm to consumers or persons involved in an electronic transaction in Namibia.

Accreditation regulations

47. The Minister may make regulations prescribing –

(a) the rights and obligations of customers of service providers and members of the public relating to the provision of accredited products and services including the provision of information or the authentication of electronic services or digital certificates;

(b) types of security services that may not be rendered or types of security products that may not be provided, unless the service, product, provider or renderer has been accredited in a specified class prescribed under section 41(2);

(c) the manner in which the Authority must administer and supervise compliance with those obligations;

(d) the procedure pertaining to the granting, suspension and revocation of accreditation;

(e) fees to be paid to the Authority in respect of anything done in terms of this Act;

(f) any matter relating to which conditions may be imposed in terms of section 45;

(g) any other matter which is necessary or expedient to prescribe for the proper implementation of this Chapter.

Offences relating to accreditation

48. A person who –

(a) holds out a service, product, renderer of a service or provider of a product to have been accredited, while that service, product, renderer or provider has not been accredited or who holds out that a service, product, renderer of a service or provider of a product has been accredited in a specific class, while that service, product, renderer or provider has not been accredited in that class;

(b) renders a service or provides a product under circumstances where the product or service must be accredited in a prescribed class, while the service or product has not been accredited in that class; or

(c) renders a service or provides a product under circumstances where the renderer of the service or the provider of the product must be accredited in a prescribed class, while he or she is not accredited in the class concerned,

commits an offence and is on conviction liable to a fine not exceeding N$50 000 or imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

CHAPTER 4
LIABILITY OF SERVICE PROVIDERS FOR UNLAWFUL MATERIAL

Definition for purposes of this Chapter

49. For the purposes of this Chapter a service provider is a person who renders –

(a) telecommunications services as contemplated in the Communications Act, 2009 (Act No. 9 of 2009) or resells such services as contemplated in that Act;

(b) any service relating to the hosting, or development of a website; or

(c) any service relating to the storage or backup of data.

Mere conduit

50. (1) A service provider is not subject to any civil or criminal liability in respect of third-party material in the form of data to which he or she merely provides access to information system services for the transmitting, routing or storage of data via an information system under his or her control, as long as the service provider –

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of

the data; and

(d) does not modify the data contained in the transmission.

(2) Transmission, routing and provision of access contemplated in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place –

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(c) for a period no longer than is reasonably necessary for the transmission.

Caching

51. (1) A service provider is not subject to any civil or criminal liability in respect of third-party material in the form of data for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider –

(a) does not modify the data;

(b) complies with conditions on access to the data;

(c) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;

(d) does not interfere with the lawful use of rights management information, widely recognised and used by industry, to obtain information on the use of the data; and

(e) removes or disables access to the data it has stored upon receiving a take down notice referred to in section 54.

Hosting

52. (1) A service provider is not subject to criminal or civil liability in respect of third-party material in the form of data where the service provider provides a service at the request of the recipient of the service that consists of the storage of data provided by a recipient of the service, as long as the service provider –

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(c) upon receipt of a take down notice referred to in section 54, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability provided for by this section do not apply to a service provider unless that service provider has designated an agent to receive notifications of infringement and has provided through its service, including on its websites in locations accessible to the public, the contact details of the agent.

(3) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

Information location tools

53. A service provider is not subject to criminal or civil liability in respect of third-party material in the form of data if the service provider refers or links users to a web page containing infringing data or an infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider –

(a) does not have actual knowledge that the data or an activity relating to the data is infringing the rights of that person;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to the reference or link to the data or activity within a reasonable time after being informed that the data or the activity relating to such data infringes the rights of a person.

Take down notice

54. (1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include –

(a) the full names and address of the complainant;

(b) the signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith; and

(h) a statement by the complainant that the information in the take down notice is to his or her knowledge true and correct.

(2) A service provider is not liable for wrongful take down in a *bona fide* response to a notification of unlawful activity which complies with subsection (1).

(3) If a service provider removes material in compliance with a take down notice, the service provider must notify the person by whom the information has been made available within three days from such take down.

(4) A person who has been notified of such take down may object to such take down by giving notice of such objection and the reason for such objection to the service provider concerned.

(5) If an objection has been received by the service provider, it must be forwarded to the person who requested the take down of the information.

(6) The person who requested the take down may provide further information to the service provider within three days from the receipt of the objection.

(7) If after the receipt of the information referred to in subsection (6) or if the period for providing that information has passed, the service provider must restore the information if he or she has a *bona fide* belief that the information may reasonably be lawful.

(8) Any person who makes a false or misleading statement in –

(a) a request for a take down notice;

(b) a notice referred to in subsection (4); or

(c) further information provided in terms of subsection (6),

commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

No general obligation to monitor

55. When providing the services contemplated in this Chapter there is no general obligation on a service provider to –

(a) monitor the data which it transmits or stores; and

(b) actively seek facts or circumstances indicating an unlawful activity.

Regulations relating to take down notices

56. The Minister may make regulations –

(a) prescribing the form of or any procedural requirement relating to notices under this Chapter;

(b) the manner and content of information to be provided by service providers in order to assist members of the public to comply with the provisions of this Chapter.

Savings

57. The provisions of this Chapter does not affect –

(a) any obligation founded on an agreement;

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

(c) an obligation imposed by a court order to remove, block or deny access to any data message or to terminate or prevent unlawful activity; and

(d) any provision in another law specifically applicable to a service provider.

CHAPTER 7
PROTECTION OF CRITICAL OR IMPORTANT DATA OR DATABASES

Identification of critical or important data and databases

58. (1) If in his or her opinion the national security, or the economic or social well-being of Namibia makes it desirable that certain data must be specially protected, must be kept specially secure or require special measures to keep it confidential, the Minister may make regulations that specify that the data or databases specified in such regulations are critical or important data or databases.

(2) Regulations made in terms of subsection (1) may identify data or databases with reference to –

(a) the type of data; or

(b) the institution or class of institution who is storing the data concerned.

(3) In respect of critical or important databases administered by public bodies, regulations contemplated in subsection (1) must be made with the concurrence of the members of the Cabinet responsible for the public bodies in question.

Registration of critical or important databases

59. (1) Regulations made in terms of section 58(1) may prescribe –

(a) the circumstances under which critical or important databases must be registered with the Ministry or such other body as may be prescribed;

(b) procedures to be followed for registration; and

(c) any other matter relating to registration.

(2) regulations made in terms of section 58(1) may provide for the maintenance of a register of critical or important databases in which the prescribed information relating to such databases must be recorded.

Management of critical or important databases

60. (1) In regulations made in terms of section 58(1) the Minister may prescribe –

(a) minimum standards for the general management of critical or important databases;

(b) any matter relating to the access to, the transfer and control of critical or important databases;

(c) rules and requirements relating to infrastructure and procedures, for securing the confidentiality, integrity and authenticity of critical and important data;

(d) procedures and technological methods to be used in the storage or archiving of critical or important data or databases;

(e) disaster recovery plans in the event of loss of critical or important databases or parts thereof;

(f) requirements and procedures with relation to the dealing with important or critical data including a prohibition of the storage of such data on certain information systems or requiring that a specified class of such data must be stored on specified information systems;

(g) which information or data stored in, or relating to critical or important databases must be regarded as confidential and under which circumstances and to whom

such information or data may or must be revealed and may also specify classes or categories of persons to which such information or data may not be revealed or who may not have access to such databases;and

(h) any other matter required for the adequate protection, management, confidentiality or control of critical or important data or databases.

(2) Regulations made in terms of section 58(1) may create offences and prescribe penalties for such offences which may not exceed a fine of N$500 000 or imprisonment for a period not exceeding five years.

Inspections

61. (1) The Minister may with the concurrence of the Prime Minister appoint a staff member in the Public Service, of the Authority or of any other institution that has as its object the security, stability or confidentiality of electronic data or information systems as the Computer Security Inspector.

(2) The Minister may appoint –

(a) additional staff members in the Public Service, of the Authority or of any other institution that has as its object the security, stability or confidentiality of electronic data or information systems, as inspectors; or

(b) a person who is not a staff member as an inspector under the conditions that he or she may determine for such purposes as he or she may determine on the recommendation of the Computer Security Inspector.

(3) The Computer Security Inspector may in writing delegate any of his or her powers to an inspector appointed under subsection (2) under such conditions and for such period as may be specified in the instrument delegating such powers.

(4) A delegation under subsection (3) may be amended or withdrawn in writing by

the Computer Security Inspector.

(5) Any power delegated under subsection (3) may still be exercised by the Computer Security Inspector.

(6) The Computer Security Inspector may, from time to time, perform inspections or evaluations of the security, stability or confidentiality of critical or important databases and the information systems on which it is stored to evaluate compliance with the provisions of this Chapter or any regulations.

(7) The Computer Security Inspector may without giving notice perform a security test on a critical database or an information system on which critical or important data is stored,or cause such test to be performed by a person that in his or her view has sufficient skill to perform the test.

(8) A security test referred to in subsection (7) may involve the access of the system without authorisation as contemplated in Chapter 8 which access is lawful and not a contravention of section 63.

(9) If an inspection or test under this section indicates that the data is not stored in a sufficiently secure manner, the computer security inspector may –

(a) refer the report to any institution that has the power to regulate the person in question for appropriate action;

(b) act in terms of subsection (10); or

(c) act in terms of paragraph(a) and (b).

(10) If the inspection or test indicates that the data is not stored in a sufficiently secure or confidential manner or that the information system in question is not sufficiently stable, the Computer Security Inspector may, after hearing the person in question, issue an order –

(a) stating the reasons for the conclusion that the data is not stored in a sufficiently secure or confidential manner or that the information system in question is not sufficiently stable;

(b) setting out the steps that are required; and

(c) specifying the time within which the steps set out in terms of paragraph (b) must be performed.

(11) If the steps referred to in subsection (10)(b) have not been taken within the time referred to in subsection (10)(c), the Computer Security Inspector may impose a fine on the institution storing the data in question, or the person responsible for the storage of the data personally, or on both the institution and the person not exceeding N$100 000.

(12) A fine imposed in terms of subsection (11) may be recovered as a debt due to the state.

CHAPTER 8
CYBERCRIME AND POWERS OF INVESTIGATION IN CRIMINAL MATTERS

Definitions

62. (1) In this Chapter, unless the context indicates otherwise, –

"access" in relation to a computer system or an information system, means to –

(a) transfer data to;

(b) obtain data from;

(c) run a program on that system (whether that program is stored on that system or is transferred to that system) or causes any program to perform any action or function or to render any data, function or action accessible to any program or person; or

(d) do anything that might reasonably have the effect that the system in question performs any action referred to in paragraph (a) to (c);

"child pornography" means the depiction by means of images, sounds, text or in any other manner of a real or imaginary person who is under the age of eighteen years, who appears to be under the age of eighteen years or who is represented or held out to be below that age (referred to in this definition as "the child") –

(a) while performing asexual act;

(b) in such a manner that it strongly suggests that the child is performing such an act or is inviting such an act;

(c) while engaging in other sexually explicit conduct where the material is calculated or appears to be calculated to stimulate erotic,sadistic or masochistic feelings or emotions:

Provided that material depicting a child who has voluntarily provided that material to another person is not child pornography, if sexual intercourse between the child depicted and the person in possession of the material would not be an offence under the law of Namibia: Provided further that material whose primary purpose is scientific, educational or artistic is not child pornography;

"forensic tool" means an investigative tool (including software or hardware) installed on or in relation to a computer system or part of a computer system which logs, stores or transmits any activity, data or any other matter relating to such a system;

"storage medium" means any article or material from which information is capable of being reproduced, with or without the aid of any other article or device.

(2) In this Chapter any action relating to a computer system or an information system is deemed to be unauthorised if –

(a) from all the facts known to the person who performs the act in question, it is reasonable to conclude that the system is not intended to be used by a member of the public or if the person belongs to a specific class of persons the system is not intended to be used by that class of persons; or

(b) the person has actual knowledge or should reasonably have known that he or she or that all members of a class to which that person belongs is not allowed to have access to that system.

(3)Access to a computer system or information system is not deemed to be unauthorised, if a system or a function of the system is accessible to the public in general, but the person who accesses the system or function did not comply with all the terms of use of the system or function: Provided that this subsection is not construed to grant any right to access the system in question.

(4) For the purposes of this Chapter it is also deemed that a person accesses a system without authorisation if he or she accesses a function of the system or data on the system which he or she is not authorised to access, although he or she might have authorisation to access other functions or data stored on the system concerned.

(5) For the purposes of this Chapter (in addition to any rule of law relating to the possession of anything)it is deemed that a person possesses data or a program, if that person –

(a) possesses a computer system or a computer storage medium on which such data or program is stored;

(b) that person has stored that data or program on an information system for the purposes of later retrieval;

(c) that program or data is stored in an information system by a third party as part of a service to store the data of the person in question.

Unauthorised access

63. Any person who accesses a computer system or an information system while he or she knows or should reasonably have known that he or she is not authorised to access the system or who accesses a system in a manner which he or she knows or should reasonably have known that he or she is not authorised to do, commits an offence and is on conviction liable to –

(a) a fine not exceeding N$100 000 or to imprisonment for a period not exceeding 10 years or to both such fine and such imprisonment; or

(b) a fine not exceeding N$1 000 000 or to imprisonment for a period not exceeding 20 years or to both such fine and such imprisonment if it is proved that –

(i) the access was for the purpose of committing fraud or theft;

(ii) the access had the effect or was calculated to cause major disruption or serious damage;

(iii) the access was for the purpose of obtaining information that is detrimental to the national security of Namibia.

Unauthorised interference

64. (1)Any person who intentionally, without authorisation performs any action that has the result or that is calculated to have the result that –

(a) computer data is altered, damaged or deteriorates;

(b) computer data is deleted;

(c) computer data is recorded wrongly;

(d) computer data is rendered inaccessible to any person or program; or

(e) the performance or effectiveness of any information system, computer system or any program running on such system deteriorates,

commits an offence.

(2) A person who commits an offence as contemplated in subsection (1) is on conviction liable to –

(a) a fine not exceeding N$100 000 or imprisonment for a period not exceeding 10 years or to both such fine and such imprisonment; or

(b) a fine not exceeding N$1 000 000 or to imprisonment for a period not exceeding 20 years or to both such fine and such imprisonment if it is proved that –

(i) the action was for the purpose of committing fraud or theft or in order to extort money from any person;

(ii) the action had the effect or was calculated to cause major disruption or serious damage;

(iii) the action was for the purpose of obtaining information that is detrimental to the national security of Namibia.

Unlawful devices, systems or programs

65. (1)Any person who intentionally creates, distributes or possesses any system, program, device or data whose purpose is to commit any offence under this Act or to perform any act contemplated in section 68 commits an offence and is on conviction liable to a fine not exceeding N$20 000or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(2) A person does not contravene subsection (1) if he or she in good faith –

(a) does research relating to the security of information systems or computer systems;

(b) is learning or teaching skills relating to the security of information systems or computer systems;

(c) is testing the security of information systems or computer systems in whose security he or she has a legitimate interest; or

(d) communicates security vulnerabilities or flaws to the public in order to promote the security of a specific information system or information systems in general.

Child pornography

66. A person who intentionally –

(a) produces child pornography for the purpose of its distribution through an information system;

(b) offers or makes available child pornography through an information system or in any other manner;

(c) distributes or transmits child pornography through an information system or in any other manner;

(d) procures or obtains child pornography through a computer system or in any other manner for himself or herself or for another person;

(e) possesses child pornography in a computer system or on a computer-data storage medium or in any other form;

(f) obtains access, through information and communication technologies or in any other manner to child pornography,

commits an offence and is on conviction liable to a fine not exceeding N$100 000 or to imprisonment for a period not exceeding 10 years or to both such fine and such imprisonment.

Electronic harassment

67. A person who intentionally posts or sends a data message, or who intentionally causes a data message to be displayed –

(a) with the intention that it causes serious emotional distress to another person;

(b) which makes credible threats of violence or other harm;

(c) which contains a statement that the accused knows to be false or with reckless disregard whether it is true or false, and with the intention to do serious harm to the reputation of another person;

(d) which makes explicit sexual suggestions knowing it to be offensive or annoying to the person to whom it is directed;

(e) contains any pictorial representation of sexual activity or nudity of a specific person –

(i) if that person has provided that information to the perpetrator privately and the person who provided that information has a reasonable expectation that the information should not be shared with other persons or the public; or

(ii) if that pictorial representation has been created by the manipulation of an image or photograph that does not depict sexual activity or nudity,

commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

Other offences

68. (1) If it is a requirement for conviction for any offence (whether under the common law or created by any law) that the accused –

(a) makes a representation;

(b) pretends to be;

(c) convinces any person;

(d) provides false information,

such a requirement is deemed to have been satisfied if the accused provides information to a computer system under circumstances where if the information had been provided to a natural person, it would have satisfied that requirement, and that information will have the effect that the system in question performs any action or allows access to any function or facility, because that system operates under the assumption that the information is correct or the representation embodied in the information is true.

(2) For the purposes of subsection (1) "providing information" includes –

(a) the use of a password, a secret code, a card or any other device which allows any person to access the system concerned, or which is used by the system to verify the identity of a person or that a person has paid for a service or otherwise obtained the right to use a service;

(b) performing any action that has the effect that the system fails to verify any matter referred to in subsection (1) or verifies such matter incorrectly.

(3) If it is a requirement for conviction for any offence (whether under the common law or created by any law) that the accused publishes or communicates anything to the public or a specific person, that requirement is deemed to have been met if –

(a) a data message has been sent to the person concerned or with the intention that it is distributed or made available to the public, as the case may be;

(b) the accused causes a data message to be displayed or made available on an information system or a computer system on which the person concerned or the public (as the case may be) can view or from which the person concerned or the public (as the case may be) can retrieve the data message .

(4) No provision of this section is construed so that a person would not be guilty of an offence if that person would have been guilty of that offence if this section had not been enacted.

Searches, seizures and forfeiture

69. (1) The provisions of Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977) are construed to relate to computer systems, computer equipment, storage media or data.

(2) The provisions of the said Chapter are construed, in so far as they relate to the seizure of data, to authorise the copying of the data, obtaining a print out of that data, or the seizure of a computer system, other computer equipment or storage medium containing that data or that can be relevant for the proof of the existence or content of that data.

(3) In addition to the powers conferred by that Chapter, a police officer also has the powers conferred by this Act.

(4) When a police officer performs any search, he or she may be assisted by any person who has special knowledge that is relevant for the search.

(5) A police officer, or a person requested by him or her may use a computer system or access a storage medium to determine any matter that is relevant for the investigation of an offence.

(6) A police officer may require any person to provide him or her with a key or password that may be necessary to perform an act referred to in subsection (5).

(7) A police officer or a person referred to in subsection (4),may require any person who possesses data or who has control over a computer system holding data that is relevant for the search in question,to assist him or her with the search.

(8) any person who without a just excuse –

(a) refuses or fails to provide a password or key as required by subsection (6);

(b) fails or refuses to render assistance as required by subsection (7); or

(c) fails or refuses to provide data in compliance with an order made under section 70(1) or fails or refuses to comply with a notice issued under section 71,

commits an offence and is on conviction liable to a fine not exceeding N$10 000 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

Production order

70. (1) If a judge or magistrate is satisfied on the basis of an application by a member of the Namibian Police that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judge or magistrate may order that a person who has access to a computer system produces from the system specified computer data or a printout or other intelligible output of that data or that such person copies that data to a storage medium.

(2) A member of the Namibian police may apply for an order under subsection (1) to a judge or magistrate in chambers without hearing any other person.

Preservation

71. (1) If a member of the Namibian police is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation might be lost, modified or destroyed, that member may issue a written notice instructing a person in control of that computer data to ensure that the data described in the notice must be preserved for the period specified in the notice which period may not be longer than seven days.

(2) A notice referred to in subsection (1) may be extended by a judge or magistrate for a period that does not exceed three months at a time.

Interception and use of forensic tool

72. (1) A member of the Namibian police may intercept communications, or utilise a forensic tool if such action is authorised by a warrant issued by a judge in chambers which warrant may be issued if the judge believes after considering information on oath that –

(a) a less intrusive method of investigation will not provide the information required;

(b) the investigation is sufficiently important and the offence is sufficiently serious to justify the method specified in the warrant; and

(c) the information sought is relevant for the investigation of an offence under this Act or any other law or the common law.

(2) A warrant issued in terms of subsection (1), must be issued without notice to the person whose communications are to be intercepted or on whose computer system a forensic tool is to be installed.

(3) A warrant issued in terms of subsection (1) must state the action authorised.

(4) A warrant issued in terms of subsection (1) is valid for the period for which it has been issued,which period may not be longer than three months, but such warrant may be

renewed on application for one or more further periods of no longer than three months at a time.

(5) An application for the issue of a warrant in terms of subsection (1) must be accompanied by a statement on oath by the applicant or any other person in which sufficient facts must be set out for the judge to decide the matters necessary to determine.

(6) If the judge considers it necessary, he or she may put any further questions to the applicant, which questions must be answered under oath by the applicant.

(7) The affidavit accompanying the application for a warrant to install a forensic tool, must explain the operation of the tool in sufficient detail to enable the judge to adequately assess the effect and operation of the tool.

(8) A warrant authorising the interception of communications, must specify which communications may be intercepted thereunder, which may be all the communications of a specified person.

(9) If a warrant authorises the installation of a forensic tool, it must state what kind of tool it authorises as well as specify on which computer system it will be installed and what method will be used to install that tool.

(10) A warrant issued in terms of subsection (1) authorises the police officer to perform all the actions stated therein.

(11) If a warrant is issued to intercept communications, it must be dealt with in terms of section (70(8) of the Communications Act, 2009 (Act No. 8 of 2009).

(12) Any person who provides telecommunications services, hosting, storage services or any other similar service to any other person must render any assistance specified in a warrant issued under this section.

(13) If it is expedient, a member of the Namibian police may be assisted by a staff

member of the Namibian Central Intelligence Service in the performance of any action authorised by a warrant issued under this section.

(14) The provisions of this section in so far as they provide for a limitation on the fundamental right to privacy contemplated in Article 13 of the Namibian Constitution, are enacted upon the authority conferred by the said Article.

Revealing particulars of investigation

73. Any person who has become aware of any order or warrant issued under this Chapter and who –

(a) reveals any particular of the order or warrant to the person against whom the investigation is conducted;

(b) performs any other act that would render the investigation less effective,

commits an offence and is on conviction liable to a fine not exceeding N$20 000 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

Co-operation with foreign authorities

74. (1) The Inspector-General of the Namibian Police may agree with any institution or body of another country to co-operate in the investigation or prosecution of an offence under this Act or an offence contemplated in section 68.

(2) If an agreement has been concluded under subsection (1) –

(a) any power of investigation provided for in this Act or the Criminal Procedure Act, 1977 (Act No. 51 of 1977) may be exercised in respect of an offence covered by the agreement as if that offence were committed in Namibia;

(b) any information obtained by an investigation in Namibia may be communi-

cated to the institution or authority in question;

(c) any information obtained from the institution or authority in question, may be used in any investigation in Namibia, and a document purporting to be an affidavit or similar declaration by a person in the country concerned may be used as supporting information to obtain a warrant or authorisation under this Act or the Criminal Procedure Act, 1977 (Act No. 51 of 1977); and

(d) despite any requirement in the law of Namibia for the authentication of documents created outside Namibia, a document created as a result of an investigation under that agreement may be used in criminal proceedings as if that document have been created inside Namibia.

Extra-territorial effect

75. For all purposes in law, an offence in terms of this Chapter is deemed to have been committed in Namibia, if –

(a) any act of preparation towards the offence or any part of the offence was performed in Namibia;

(b) the offence was committed on a ship or aircraft registered in Namibia;

(c) the offence was committed by a citizen of Namibia; or

(d) an information system in Namibia was affected by the offence or any person in Namibia suffered loss, damage to property or any other disadvantage or infringement of his or her rights as a result of the offence.

CHAPTER 9
MISCELLANEOUS MATTERS

Regulations

76. (1) The Minister may make regulations relating to any matter that may or must be prescribed and to any matter that is reasonably necessary or expedient to be prescribed to achieve the objects of this Act.

(2)The provisions of section 18(4) apply to regulations made under this Act.

(3) When the Minister intends to make regulations under this Act, he or she may instruct the Authority to conduct a rule-making procedure in terms of the Communications Act, 2009 (Act No. 8 of 2009).

Repeal and amendment of laws

77. (1) The Computer Evidence Act, 1985 (Act No. 32 of 1985) is repealed.

(2) Section 75 of the Communications Act, 2009 (Act No. 8 of 2009) is amended by the insertion in paragraph (d) of the following subparagraphs after subparagraph (i):

"(iA) subject to any procedural requirements that may be prescribed and any other law, information that is necessary to investigate an offence;

(iB) the information is required because it is necessary to locate a person and it is necessary to locate the person concerned in the public interest, the national interest of Namibia or for the purposes of a criminal investigation or in the interest of the missing person;

(iC) where the person concerned has consented or where it is reasonable under the circumstances to assume that the person would have consented and it is due to the urgency of the request or for another reason not possible to obtain the consent of the person concerned: Provided that a general consent in a contract is not valid consent for the purposes of this subparagraph;".

Short title and commencement

78. (1) This Act is called the Electronic Transactions and Cybercrime Act, 2016, and comes into operation on a date determined by the Minister by notice in the *Gazette*.

(2) Different dates may be determined under subsection (1) for different provisions of this Act.