The Electronic Transactions Act, 2063 (2008)

Date of Authentication and Publication

22 Mansir 2063 (december 8, 2006)

Act number 27 of the year 2063

An Act promulgated for Electronic Transactions

Preamble:

WHEREAS, it is expedient to make, legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured;

And where as, for controlling the acts of unauthorized use of electronic records or of making alteration in such records through the illegal manner,

Now, therefore, be it enacted by the House of Representatives in the First Year of the issuance of the Proclamation of the House of Representatives, 2063(2007) .

Chapter - 1

Preliminary

1. **Short Title, Extension and Commencement:** (1) This Act may be called "The Electronic Transactions act,2063 (2008)".

(2) This Act shall be deemed to have been commenced from 24 Bhadra 2063 (sep.2, 2006).

(3) This Act shall extend throughout Nepal and shall also apply to any person residing anywhere by committing an offence in contravention to this Act.

2. **Definitions:** Unless the subject or context otherwise requires, in this Act,-

(a) "Asymmetric Crypto System" means a system that creates a secured key-pair consisting of a private key creating a digital signature and a public key to verify the digital signature.

(b) "License" means a license obtained pursuant to Sub-section (3) of Section 18.

(c) "Originator" means a person who generates, stores or transmits electronic records, and this term also includes a person who causes any other person to carry out such functions:

Provided that it shall not include an intermediary.

(d) "Computer" means an electro-magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic and memory functions by manipulating electro-magnetic or optical impulses, and also includes all acts of input, output, processing, storage and computer software or communication facilities which are connected or related to the computer in any computer system or computer network.

(e) "Computer Database" means an information, knowledge and concept or presentation of instructions, which are being prepared or have already been prepared in word, image, voice or audio visual form in a formalized manner or which have been produced by a computer, computer system or computer network, with a view to use in a computer, computer system or computer network.

(f) "Computer Network" means an interrelationship between two or more than two computers having interconnection with each other or in contact of communication.

(g) "Computer System" means a device or a group of devices, containing all computer programmes including input and output support devices, electronic instructions, input and output data that performs logical, arithmetic, data storage and retrieval, communication including controlling functions.

(h) "Computer Resource" means a computer, computer system, computer network, data, computer database or software.

(i) "Subscriber" means a person who has obtained a certificate under Sub-section (3) of Section 31.

(j) "Key Pair" means a private key in an asymmetric crypto system and of pair of public key, interconnected in a mathematics form with the private key which has a code to verify digital signature by the public key to be created from the private key.

(k) "Data" means the presentation of information, knowledge, fact and concept or instructions in any form, which are kept in a formalized manner in a computer system or computer network and is intended for processing the same, or processed or stored in a computer memory.

(l) "Tribunal" means the Information Technology Tribunal formed pursuant to section 60.

(m) "Private Key" means a key of any key pair used to create a digital signature.

(n) "Controller" means the Controller appointed or designated pursuant to section 13.

(o) "Digital Signature" means a signature made in any electronic form to be included in the transformation of electronic record by a person having a non- transformed initial electronic record and the public key of signatory by using a type of asymmetric crypto system that may clearly ascertain the following matters:

(1) Whether or not transformation of electronic record was created by using a type of private key keeping a logical consistency with the public key of signatory; and

(2) Whether or not the initial electronic record has been changed after the transformation of electronic record.

(p) "Access" means an opportunity of gaining entry into, logical, arithmetical or resources of memory function of any computer, computer system or computer network, giving instructions to such resources or making communication contact with such resources.

(q) "Appellate Tribunal" means the Information Technology Appellate Tribunal formed pursuant to section 66.

(r) "Certificate" means a Digital Signature Certificate issued by the Certifying Authority under Section 30.

(s) "Certification Practice Statement" means any statement issued by a Certifying Authority to specify the practices to be applied by the Certifying Authority while issuing a Digital Signature Certificate.

(t) "Certifying Authority" means a certifying authority which has obtained a license to issue a Digital Signature Certificate under Sub-section (3) of Section 18.

(u) "Addressee" means a person receiving the processed electronic record as intended by the originator.

Provided that it shall not include an intermediary.

(v) "Electronic Record" means the data, record, image or sound transmitted, received or stored in an electronic form by generating the same through any means.

(w) "Electronic Form" means a form of information transmitted, received or stored by generating the same through the means of magnetic, optical, computer memory or similar other devices.

(x) "Public Key" means a key of any key pair used to verify digital signature.

(y) "Information" means the data details of the scripted texts, images, sounds, codes, computer programmes, software and computer databases.

(z) "Information system" means a system to generate, produce, transmit, receive, store and display information or to process the same by other method.

(aa) Software" means any specific part of computer system such as system software and application software having the capacity for operating computer hardware.

(ab) "Computer Accessory" means a technology such as computer resource, the information used by any institution in its business, a software-like item produced or purchased by such an institution, hardware and computer network.

(ac) "Government Authority" means a Ministry, Secretariat, Department of Government of Nepal or the Offices thereunder, Constitutional Body or the Offices thereunder, Court or Tribunal or Office of the Nepal Army and it shall also includes other Offices of the similar nature.

(ad) "Public Institution" means the following institutions:-

(1) A company, bank or board whether fully or partially owned or controlled by Government of Nepal , or a Commission agency, authority, corporation, enterprise board, centre, council and other corporate body of the similar nature established by Government of Nepal pursuant to the laws prevailing.

(2) A university, school, research centre, and other similar academic or educational institutions operated by Government of Nepal or which have been receiving a full or partial grant from Government of Nepal,

(3) The Local Bodies formed under the Local Self-Governance Act, 1998 (2055 B.S);

(4) The Institutions run on the loan, grant or guarantee of Government of Nepal;

(5) The Institution which is fully or partially owned or controlled by the institution referred to in sub-Clauses (1), (2), (3) or (4) or which receiving grant from such institution;

(6) Any other Institutions prescribed by Government of Nepal as a public institution by a notification published in the Nepal Gazette.

(ae) "Prescribed" or "As prescribed" means prescribed or as prescribed in Rules framed under this Act.

Chapter - 2

Provisions Relating to Electronic Record and Digital Signature

3. Authencity of Electronic Record: (1) Any subscriber may, subject to the provisions of this section, authenticate to any electronic record by his/her personal digital signature.

(2) While authenticating the electronic record pursuant to Sub-section (1), an act of transforming such electronic record to other electronic record shall be effected by the use of asymmetric crypto system and hash function.

Explanation: For the purpose of this section, "hash function" means the acts of mapping of algorithm or translating of a sequence of bits into another, generally smaller, set yielding the same hash result from any record in the same form while executing the algorithm each and every time by using the same record as an input, infeasible to derive or reconstruct any record from the hash result produced by the algorithm from the computation point of view, and making the two records, which produce the same hash result by using the algorithm, computationally infeasible to derive.

(3) Any person may verify the electronic record by using the public key of the subscriber.

4. **Legal Recognition of Electronic Record:** Where the prevailing law requires any information, documents, records or any other matters to be kept in written or printed typewritten form, then, if such information, document, record or the matter is maintained in an electronic form by fulfilling the procedures as stipulated in this Act or the Rules made hereunder, such electronic record shall also have legal validity.

5. **Legal Recognition of Digital Signature:** Where the prevailing law requires any information, document, record or any other matters to be certified by affixing signature or any document to be signed by any person; then, if such information, documents, records or matters are certified by the digital signature after fulfilling the procedures as stipulated in this Act or the Rules made hereunder, such digital signature shall also have legal validity.

6. **Electronic Records to be Kept Safely:** Where the prevailing law requires any information, document or record to be kept safely for any specific period of time and if such information, document or record are kept safely in an electronic form, by fulfilling the following condition,, such information, document or record shall have legal validity if that is,-

(a) kept in an accessible condition making available for a subsequent reference,

(b) kept safely in the format that can be demonstrated subject to presenting again exactly in the same format in which they were originally generated and transmitted or received or stored,

(c) kept making the details available by which the origin, destination and transmission or date and time of receipt can be identified,

Provided that the provision of this Clause shall not be applied in regard to any information to be generated automatically for the purpose of transmitting or receiving any record.

7. **Electronic Record May Fulfill the Requirement of Submission of any Original Document:** Where the prevailing law requires that any record shall

have to be submitted or retained in its main or original form or kept safely, then, such requirement shall, if the following terms are fulfilled, be deemed to have been satisfied by the electronic records:

(a) If there exits a ground as prescribed that can be believed that any type of change is not made in such record by any means from the fist time of its generation in electronics form,

(b) If such record is of the nature where there is a compulsion of submitting such document to any person it could be clearly shown to such a person to whom it requires to do so.

8. **Secured Electronic Records:** If the verification has been made as prescribed in connection with the matter as to whether or not any type of changes are made into the electronic records generated with the application of security procedures as prescribed, such electronic records shall be deemed to be a secured electronic records.

9. **Secured Digital Signature:** Where any digital signature made in electronic record has been examined in a manner as prescribed with the application of such security procedure as prescribed, then, such digital signature shall be deemed to be a secured digital signature.

Chapter - 3

Provision Relating to Dispatch, Receipt and Acknowledgement of Electronic Records

10. **Electronic Record to be Attributed to Originator:** (1) Any specific electronic record shall, in case of any of the following conditions, be attributed to the originator:

(a) If such an electronic record was transmitted by the originator him/herself,

(b) If such an electronic record was transmitted by a person who had the authority to act on behalf of the originator in respect of such an electronic record,

(c) Such an electronic record was transmitted through any information system that was programmed by the originator or on behalf of the originator to operate automatically.

(2) If any condition exists as prescribed in respect of electronic record transmitted pursuant to Sub-section (1), the addressee shall assume that such an electronic record is attributed to any particular originator and shall have the authority to act thereon accordingly.

11. <u>Procedure of Receipt and Acknowledgement of Electronic Record:</u>

(1) Where the originator requests the addressee to transmit the acknowledgement or receipt of electronic record at the time of or before the dispatch of such electronic record or where there is an agreement between the originator and addressee to transmit the acknowledgement or receipt of such an electronic record, then, the provisions of Sub-sections (2), (3) and (4) shall be applied in relation to the receipt and acknowledgement of such an electronic record.

(2) Where there is no agreement between the originator and addressee that information or acknowledgement of receipt of electronic record is to be given in a particular format or by a particular manner, such an information or receipt may be given as the following:-

(a) by automated or any other means of communication by the addressee,

(b) by any conduct of the addressee sufficient to indicate that the originator has received electronic record.

(3) Where the originator has stipulated in relation to any electronic record that such an electronic record shall be binding on him/her only after the receipt of information or acknowledgement of receipt of such electronic record

from the addressee, then, unless the information or acknowledgement of receipt of such an electronic record has been so received from addressee, the electronic record shall not be deemed to have been transmitted by the originator.

(4) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and where the originator and addressee have not agreed upon or have not specified any time for acknowledgement of such receipt of electronic record, then, the originator shall have to receive such acknowledgement of receipt of such an electronic record from addressee within a specified time as prescribed. If such acknowledgement of receipt is not received from addressee, then, such an electronic record shall be deemed to have not been transmitted by the originator.

(5) Other procedures of receipt of acknowledgement of electronic record shall be as prescribed.

12. **Time and Place of Dispatch and Receipt of Electronic Record:** (1) Save as otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters into an information system outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as prescribed.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record shall be deemed to have been dispatched from the place where the originator has his/her place of business and shall be deemed to have been received at the place where the addressee has his/her place of business.

Explanation: For the purpose of this Sub-section "the place of business" means:

(a) In case the originator or the addressee has more than one place of business, the place of business means the place where the concerned business shall be operated

(b) If the originator or the addressee does not have a place of business, their place of residence shall be considered their place of business.

Chapter 4

Provisions Relating to Controller and Certifying Authority:

13. Appointment of the Controller and other Employees: (1) Government of Nepal may, by notification in the Nepal Gazette, designate any Government officer or appoint any person who has qualifications as prescribed in the office of the Controller.

(2) Government of Nepal may, in order to assist the Controller to perform his/her functions to be performed under this Act, appoint or assign a Deputy Controller and other employees as required. The employees so appointed or assigned shall perform their functions under the general direction and control of the Controller.

14. Functions, Duties and Powers of the Controller:

The functions, duties and powers of the controller shall be as follows:-

(a) To issue a license to the certifying Authority,

(b) To exercise the supervision and monitoring over the activities of Certifying Authority,

(c) To fix the standards to be maintained by certifying authority in respect to the verification of digital signature,

(d) To specify the conditions to be complied with by the certifying authority in operating his/her business,

(e) To specify the format of the certificate and contents to be included therein,

(f) To specify the procedures to be followed by the certifying authority while conducting his/her dealings with the subscribers,

(g) To maintain a record of information disclosed by the certifying authority under this act and to make provision of computer database accessible to public and to update such database,

(h) To perform such other functions as prescribed.

15. **License to be obtained:** No person shall perform or cause to be performed the functions of a certifying authority without obtaining a license under this Act.

16. **Application to be submitted for a License:** (1) Any person willing to work as Certifying Authority by issuing a certificate under this Act and who has the qualifications as prescribed shall have to submit an application to the controller in a format as prescribed accompanied by a fee as prescribed for obtaining a license for the certification.

(2) The applicant applying under Sub-section (1) shall also attach the following documents:

(a) Details regarding certification,

(b) Documents to prove the identification and verification of the applicant,

(c) Statements specifying the financial resources, human resources and other necessary facilities,

(d) Such other documents as prescribed.

(3) The controller may, if he/she thinks necessary, ask the applicant to serve additional documents and details in connection to examine the appropriation of the applicant as to perform the function of Certifying Authority. If the necessary additional documents and details are so asked, no actions shall be taken upon the application of the applicant unless he/she submits such documents and details.

17. **Other Functions and Duties of the Certifying Authority**:

Other functions and duties of the certifying authority, other than those to issue a certificate, to suspend or revoke it, shall be as prescribed.

18. **Procedure for granting of a license**: (1) The Controller may, on receipt of an application under section 16, after considering the qualification of applicant and also the documents and statements decide upon within a period of two months of receipt of such application whether or not such a person possesses the financial, physical and human resources, and other facilities as prescribed and whether or not a license should be issued to such an applicant and a notice to that effect shall be given to him.

(2) While deciding upon the issuance of a license under Sub-section (1), the Controller may inspect the facilities, financial and physical resources of the applicant.

(3) If the Controller decides to issue a license under Sub-section (1), a license in the prescribed format shall be issued to the applicant specifying the period of validity of the license and also the terms and conditions to be followed by him.

(4) Other procedures relating to the issuance of a license shall be as prescribed.

19. **Renewal of License:** (1) A license obtained by Certifying Authority shall have to renew in each year,

(2) A Certifying Authority desirous to renew the license under Sub-section (1), shall have to submit and application in the prescribed format to the Controller at least two months prior to the expiry of the period of validity of such a license along with such renewal fee as prescribed,

(3) If an application is submitted for renewal, under Sub-section (2), the Controller shall have to decide whether to renew the license or not, after completing the procedures as prescribed one month prior to the expiry date of validity of such a license,

(4) While deciding to reject to renew a license, the applicant shall be given a reasonable opportunity to present his/her statement in this regard.

20. **License may be suspended:** (1) If the documents or statement and statement of financial and physical resources submitted by the certifying authority before the Controller in order to obtain a license are found incorrect or false or the conditions to be complied with in course of operation of business is not complied with or this Act of the Rules framed hereunder are found to be violated, the Controller may suspend the license of the certifying authority till the inquiry in this regard is completed.

Provided that, Certifying Authority shall be given the reasonable opportunity to present his/her defense prior to such suspension of a license.

(2) Other procedures concerning suspension of license and other provisions related thereto be as prescribed.

21. **License may be revoked:** (1) If the controller believes, after completion of an inquiry in connection to any activity of Certifying Authority, made duly, as prescribed, that any of the following circumstances have been occurred, the Controller may revoke a license issued under this Act, at any time, as he deems to be appropriate:

(a) If the Certifying Authority fails to comply with the liabilities under this act and the rules made thereunder.

(b) If it is found that the Certifying Authority has submitted false or incorrect document or statement at the time of submitting an application for obtaining a license or for its renewal, as the case may be.

(c) If the Certifying Authority operates business in such a manner so that it shall make adverse effect to the public interest or to the national economy,

(d) If the Certifying Authority commits any act that is defined as an offence under this Act or the Rules framed hereunder.

(2) The Controller shall, prior to revocation of a license under Sub-section (1), provide a reasonable opportunity to the Certifying Authority to present his/her defense.

(3) Other procedures concerning revocation of a license shall be as prescribed.

22. **Notice of Suspension or revocation of a License:** (1) Where a license of any Certifying Authority is suspended or revoked under Section 20 or 21, as the case may be the Controller shall give a written notice to the Certifying Authority of such suspension or revocation, as the case may be, to such a certifying Authority and shall keep such a notice in his computer database and also publish in the electronic form.

(2) The Controller shall publish the notice of suspension or revocation of a license at least in two daily newspapers in Nepali and English languages for two times.

Provided that, there shall be no effect to any decision of suspension or revocation, as the case may be, made by the Controller under Section 20 or 21, merely on the ground of non-publication of such a notice.

23. **Recognition to Foreign Certifying Authority may be given:** (1) The Controller may with the prior approval of Government of Nepal, and subject to such conditions and restrictions as may be prescribed, by notification in the Nepal Gazette, recognize any Certifying Authority who has obtained a license to certify under any foreign law. Any foreign Certifying Authority so recognized may issue the certificates under this Act or the Rules made thereunder throughout the Nepal.

(2) The procedures to be adopted in providing the recognition to a foreign Certifying Authority as referred to in Sub-section (1), shall be as prescribed.

24. **The Controller may issue Orders:** (1) The Controller may, in order to cause to fulfill the responsibilities in regard to issuance of a certificate by the

Certifying Authorities, issue directives, from time to time. It shall be a duty of the Certifying Authority to comply with such directives.

25. **The Controller may delegate power:** The Controller may, in order to perform the function to be performed by him/her delegate to any officer subordinate to him/her to exercise all or any of his/her powers under this Act or the Rules framed thereunder.

26. **The Controller may investigate:** (1) The Controller may, if he/she believes that this Act or the Rules framed hereunder are not complied with by the Certifying Authority or by other concerned person, conduct him/herself or cause any officer to conduct necessary investigation in that regard.

(2) It shall be a duty of Certifying Authority to assist the investigations, referred to in Sub-section (1).

(3) The procedure to be followed by the Controller or any other officer in respect to investigation referred to in Sub-section (1) shall be as prescribed.

27. **Performance Audit of Certifying Authority:** (1) The Controller may conduct or cause to be conducted performance audit of the Certifying Authority in each year.

(2) The Controller may, for the purpose of the performance audit referred to in Sub-section (1), appoint any recognized auditor, who has expertise in computer security or any computer expert.

(3) The Controller shall publish the report of the performance audit in the electronic form made under Sub-section (1) by maintaining in his/her computer database.

(4) The qualification of the performance auditor or remuneration and the procedures of such audit shall be as prescribed.

(5) The Controller shall fix the standard of the service of Certifying Authority and publish a notice thereof publicly for the information to the public-in-general.

28. **The Controller to have the Access to Computers and data:** (1) The Controller shall, if there is a reasonable ground to suspect that provision of this Act and Rules framed hereunder has been violated, have the power to have the access to any computer system, apparatus, devices, data, information system or any other materials connected with such system.

(2) The Controller may, for the purpose of Sub-section (1), issue necessary directives to the owner of any computer system, apparatus, device, data, information system or any material connected with such system or to any other responsible person to provide technical or other cooperation as he/she deems necessary.

(3) It shall be the duty of the concerned person to comply with such directive issued under Sub-section (2).

29. **Record to be maintained:** (1) The Controller shall maintain records of all Certificates issued under this Act.

(2) The Controller shall, in order to ensure the privacy and security of the digital signatures, perform following functions:

(a) To use Computer Security System,

(b) To apply security procedures to ensure the privacy and integrity of digital signature,

(c) To comply with the standard as prescribed,

(3) The Controller shall maintain and update computerized data base of all public keys in a computer system.

(4) For the purpose of verification of Digital Signature, the Controller shall make available a public key to any person requesting for such a key.

Chapter-5

Provisions Relating to Digital Signature and Certificates

30. **Certifying Authority may issue a Certificate:** Only a licensed or recognized Certifying Authority under this Act may issue a Digital Signature Certificate.

31. **Apply to obtain a Certificate:** (1) Any person desirous to obtain Digital Signature Certificate may apply to the Certifying Authority in such a format along with such fee and other statements as prescribed.

(2) On receipt of an application under Sub-section (1), the Certifying Authority shall have to decide whether to issue or not a certificate to the applicant within one month of such application so received.

(3) The Certifying Authority shall, if it decides to issue a certificate under Sub-section (2), issue a Digital Signature Certificate within seven days affixing his signature in a prescribed format with the inclusion of such statements as prescribe and if it decides to reject to issue such certificate, the applicant shall be notified the reasons for rejection within seven days.

32. **Certificate may be suspended:** (1) Certifying Authority may suspend the Certificate in following circumstances:

(d) If the subscriber obtaining the certificate or any person authorized to act on behalf of such a subscriber, requests to suspend the certificate.

(e) If it is found necessary to suspend the certificate that contravenes public interest as prescribed.

(f) If it is found that significant loss might be caused to those persons who depend on the certificate by the reason that provisions of this Act or the Rules framed hereunder were not followed at the time of issuance of the certificate, and if

the controller instructs to suspend the certificate having specified the above ground.

(2) Grounds and procedures for suspension and release of the suspended certificates shall be as prescribed.

33. **<u>Certificate may be revoked:</u>** (1) The Controller or the Certifying Authority may revoke a Certificate in following conditions:

(g) Where the subscriber or any other person authorized by him requests to revoke a certificate,

(h) If it is necessary to revoke in a certificate that contravenes the public interest as prescribed,

(i) Upon the death of the subscriber,

(j) Upon the insolvency, winding up or dissolution of the company or corporate body under the prevailing laws, where the subscriber is a company or a corporate body.

(k) If it is proved that a requirement for issuance of the Certificate was not satisfied.

(l) If a material fact represented in the certificate is proved to be false.

(m) If a key used to generate key pair or security system was compromised in a manner that affects materially the Certificate's reliability.

(2) The procedures to be followed by the Controller or Certifying Authority with respect to revocation of a Certificate shall be as prescribed.

34. **<u>Notice of Suspension or Revocation:</u>** (1) Where a Certificate is suspended or revoked under sections 32 or 33, the Certifying Authority or the Controller, as the case may be, shall publish a public notice thereof maintaining its record in their repository.

(2) It shall be the responsibility of the Certifying Authority or the Controller, as the case may be, to communicate the subscribers as soon as possible on suspension or revocation Certificates.

Chapter-6

Functions, Duties and Rights of Subscriber

35. **To Generate Key pair:** (1) Where any Certificate issued by the Certifying Authority and accepted by subscriber, consisting of a public key which corresponds to the key pair and to be listed in such Certificate and if such key pair is supposed to be generated by the subscriber only, then the subscriber shall generate such key pair by applying the secured asymmetric crypto system.

(2) Notwithstanding anything contained in Sub-section (1), if a Certifying Authority and the subscriber have concluded an agreement or the Certifying Authority has accepted any specific system regarding the security system to be used to generate the key pair, then, it shall be the duty of subscriber to apply the security system as specified in agreement or accepted by the Certifying Authority.

36. **To Accept a Certificate:** (1) The certificate shall be deemed to have been accepted by the subscriber in the following conditions:

(n) If he publishes such a certificate or authorizes to publish to one or more persons, or

(o) If there exists any ground of his acceptance to such certificate which may cause to believe it.

(2) If the certificate is accepted it shall be deemed that the subscriber, by that reason, has guaranteed to all who reasonably rely on the information contained in the certificate that-

(a) The subscriber holds the private key corresponding to the public key and is entitled to hold the same,

(b) All representations and information made by the subscriber to the Certifying Authority in course of issuance of the certificate are true and correct and all facts relevant to the information contained in the certificate are true, and

(c) All information mentioned in the certificate is, to the best knowledge of subscriber, is true and correct.

37. <u>To retain the private key in a secured manner</u>: (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in the Certificate and adopt all measures to prevent its disclosure to a person not authorized to affix the digital signature of subscriber.

(2) If the private key has been disclosed or compromised by any reason whatsoever, then, the subscriber shall communicate the same without any delay to the Certifying Authority and on receipt of such information the Certifying Authority shall immediately suspend such a Certificate.

(3) If a certificate is suspended under this Act, it shall be a duty of the subscriber to retain the private key under this section in a safe manner throughout the duration of such suspension of Certificate.

38. <u>To Deposit the Private Key to the Controller</u>: (1) If the Controller thinks, in order to protect the sovereignty or integrity of Nepal, to maintain the friendly relations with friendly countries, to maintain the law and order, to prevent from committing of any offence under the laws prevailing, and or in other conditions as prescribed, necessary to issue an order to any subscriber to deposit the private key to him/her specifying reason there for, such a subscriber shall immediately deposit the private key to the Controller.

(2) The controller shall not inform any unauthorized person about the private key deposited as per sub section (1).

Chapter-7

Electronic Record and Government use of Digital Signature

39. Government Documents may be published in electronic form: (1) Government of Nepal may also publish ordinance, Act, Rules Bye-laws, Formation Orders or notifications or any other matters in the electronic form which are published in the Nepal Gazette under the prevailing laws.

(2) Where the prevailing law provides for the filing of any form, application or any other document or any record to be generated or retained or secured and or any license or permit or approval or certificate to be issued or provided or any payment to be made in any Government agency, or public entity or in any bank or financial institution operating business within the Nepal, it may be filed, generated, retained or secured or issued or granted in electronic form or payment may be made in electronic mode of communication, and, it shall not be denied to provide the legal validity to such form, application, document record, license, permit or approval, certificate or payment on the ground of the use of electronic form or electronic communication mode.

40. To Accept the Document in Electronic Form: (1) Government agency or public entity or bank or financial institutions operating business within the Nepal may also accept any document and payment to be submitted or paid to them under the prevailing law in electronic form or through any electronic mode and if such documents and submitted or payment is made, as the case may be, it shall not be denied to grant legal recognition merely on the ground that it was accepted electronic form or through any electronic mode.

(2) Notwithstanding anything contained in Sub-section (1) no Government agency or public entity or bank of financial institution operating business within the Nepal shall, except in the conditions as prescribed and government agencies as prescribed, be compelled to accept any document or

payment in electronic form, and such an agency or institution shall, except in the conditions and agency as prescribed, not compel to any other persons to accept any document in electronic form or the payment through any electronic form.

(3) For the purpose of Sub-section (1), the provision relating to the procedure, process and format to be followed shall as prescribed.

41. **Use of Digital Signature in Government Offices:** (1) Where it is required that the concerned person shall have to affix his/her signature in any document or record for verification of such document or record to be transmitted or issued by any Government agency or public entity or bank or financial institution operating business within the Nepal or to be accepted by such agency or institution then, Government of Nepal may, if it thinks appropriate, make a provision to use digital signature instead of such a signature.

(2) Notwithstanding anything contained elsewhere in this Act, Government of Nepal may, for the purpose of the provision made in Sub-section (1), prescribe additional security procedure for the verification and authentication of such digital signature.

(3) Provisions regarding the Certifying Authority and Digital Signature Certificate to be used by the government agency or entity referred to in Sub-section (1), shall be as prescribed.

Chapter –8

Provisions Relating to Network Service

42. **Liability of Network Service Providers:** Intermediaries providing their services as network service providers shall undertake the following liabilities in regard to such service provided by them:

(a) Liabilities referred to in the agreement made with the subscriber in regard to service provision,.

(b) Liabilities referred to in the license of network service providers, and,

(c) Any such other liability as prescribed.

43. **Network Service Provider not to be Liable:** Notwithstanding anything contained in Section 42, no network service provider shall be liable to bear any criminal or civil liability arising from any fact or statement mentioned or included in the information or data of the third party made available in electronic form by him/her merely on the ground that he/she has made available the access to such information or data.

Provided that, such a person or institution providing network service shall not be relieved from such liability, if he/she has made available access to such information or data with the knowledge that any fact or statement mentioned or included in such information or data contravene this Act or Rules framed hereunder.

Explanation: For the purpose of this section" Third Party" means a net work service provider who provides service as intermediary and any person over whom there is no control of the network service provider.

Chapter -9

Offence Relating To Computer

44. **To Pirate, Destroy or Alter computer source code:** When computer source code is required to be kept as it is position for the time being the prevailing law, if any person, knowingly or with malafide intention, pirates, destroys, alters computer sources code to be used for any computer, computer programme, computer system or computer network or cause, other to do so, he/she shall be liable to the punishment with imprisonment not exceeding three years or with a fine not exceeding two hundred thousand Rupees or with both.

Explanation: For the purpose of this section "computer source code" means the listing of programmes, computer command, computer design and layout and programme analysis of the computer resource in any form.

45. **Unauthorized Access in Computer Materials:** If any person with an intention to have access in any programme, information or data of any computer, uses such a computer without authorization of the owner of or the person responsible for such a computer or even in the case of authorization, performs any act with an intention to have access in any programme, information or data contrary to from such authorization, such a person shall be liable to the punishment with the fine not exceeding Two Hundred Thousand Rupees or with imprisonment not exceeding three years or with both depending on the seriousness of the offence.

46. **Damage to any Computer and Information System:** If any person knowingly and with a *mala fide* intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or affects it injuriously or causes any person to carryout such an act, such a person shall be liable to the punishment with the fine not exceeding two thousand Rupees and with imprisonment not exceeding three years or with both.

47. **Publication of illegal materials in electronic form:** (1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both.

(2) If any person commit an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment.

48. **Confidentiality to Divulge:** Save otherwise provided for in this Act or Rules framed hereunder or for in the prevailing law, if any person who has an access in any record, book, register, correspondence, information, documents or any other material under the authority conferred under this Act or Rules framed hereunder divulges or causes to divulge confidentiality of such record, books, registers, correspondence, information, documents or materials to any unauthorized person, he/she shall be liable to the punishment with a fine not exceeding Ten Thousands Rupees or with imprisonment not exceeding two years or with both, depending on the degree of the offence.

49. **To inform False statement:** If any person with an intention to obtain a license from Certifying Authority under this Act or with any other intention either to Controller or with an intention to obtain Digital Signature Certificate or with any other intention conceals statement knowingly or lies any statement to be submitted to the Certifying Authority any false statements shall be liable to the punishment with a fine not exceeding One Hundred Thousands rupees or with an imprisonment not exceeding two years or with both.

50. **Submission or Display of False License or Certificates:** (1) If any person who works as a Certifying Authority without a license issued by the Controller under this Act, shall be liable to the punishment with a fine not exceeding one hundred thousands Rupees or with an imprisonment not exceeding two years or with both, depending on seriousness of the offence.

(2) Any person without obtaining a license from the Certifying Authority publishes a fake license or false statement in regard to license or provides to any person by any other means, shall be liable to the punishment not exceeding one hundred thousand Rupees in the case where the act referred to in Sub-section (1) has not been accomplished by such a person.

(3) If any person publishes or otherwise makes available a certificate to any other person by any means knowingly that a certificate is not issued by the Certifying Authority referred to in such a certificate or the subscriber listed in such certificate has not accepted the certificate or such a certificate is already

suspended or revoked, shall be liable to the punishment with a fine not exceeding one hundred thousands Rupees or with an imprisonment not exceeding two years or with both.

Provided that, if such a certificate suspended or revoked is published or provided for the purpose of verification of the Digital Signature before it was suspended or revoked, it shall not be deemed to have been committed an offence under this Sub-section.

51. **Non-submission of Prescribed Statements or Documents:** (1) If any person responsible to submit any statement, document or report to the Controller or Certifying Authority under this Act or Rules framed hereunder, fails to submit such statement, document, or report within the specified time limit, such a person shall be liable to the punishment with a fine not exceeding fifty thousands Rupees.

(2) Any person who fails to maintain duly any book, register, records or account and in a secured manner to be maintained duly and in a secured manner under this Act or Rules framed hereunder shall be liable to the punishment with a fine not exceeding fifty thousands Rupees.

52. **To commit computer fraud:** If any person, with an intention to commit any fraud or any other illegal act, creates, publishes or otherwise provides digital signature certificate or acquires benefit from the payment of any bill, balance amount of any one's account, any inventory or ATM card in connivance of or otherwise by committing any fraud, amount of the financial benefit so acquired shall be recovered from the offender and be given to the person concerned and such an offender shall be liable to the punishment with a fine not exceeding one hundred thousand Rupees or with an imprisonment not exceeding two years or with both.

53. **Abetment to commit computer related offence:** A person who abets other to commit an offence relating to computer under this Act or who attempts or is involved in the conspiracy to commit such an offence shall be liable to the

punishment with a fine not exceeding fifty thousand Rupees or with imprisonment not exceeding six months or with both, depending on the degree of the offence.

54. **Punishment to the Accomplice:** A person who assists others to commit any offence under this Act or acts as accomplice, by any means shall be liable to one half of the punishment for which the principal is liable.

55. **Punishment in an offence committed outside Nepal:** Notwithstanding anything contained in the prevailing laws, if any person commits any act which constitutes an offence under this Act and which involves the computer, computer system or computer network system located in Nepal, even though such an act is committed while residing outside Nepal, a case may be filed against such a person and shall be punished accordingly.

56. **Confiscation:** Any computer, computer system, floppy, compact disks, tape drivers, softwares or any other accessory devices used to commit any act deemed to be an offence relating to computer under this Act shall be liable to confiscation.

57. **Offences Committed by a corporate body:** (1) If any act is done by a corporate body which deems an offence under this Act, such an offence shall be deemed to have been committed by a person who was responsible as chief for the operation of the corporate body at the time of committing such an offence.

Provided that, if the person who was responsible as a chief for the operation of such a corporate body proves that such an offence was committed without his/her knowledge or that he/she exercised all reasonable efforts to prevent such an offence, he/she shall not be liable to the guilty.

(2) Notwithstanding anything contained in Sub-section (1), if it is proved that any offence under this Act committed by a corporate body with the consent or in knowledge or by the reason of negligence of a director, manager, secretary or any other responsible person of such corporate body, such an

offence shall be deemed to have been committed by such a corporate body and by a director, manager, secretary or other responsible person of such a corporate body.

58. **Other Punishment:** If any violation of this Act or Rules framed hereunder has been committed, for which no penalty has been separately provided, such a violator shall be liable to the punishment with a fine not exceeding fifty thousand Rupees, or with an imprisonment not exceeding six months or with both.

59. **No Hindrance to Punish Under the Laws prevailing:** If any act deemed to be an offence under this Act shall also be deemed to be another offence under the laws prevailing, it shall not be deemed to have been hindered by this Act to file a separate case and punish accordingly.

Chapter-10

Provisions Relating to Information Technology Tribunal

60. **Constitution of a Tribunal:** (1) Government of Nepal shall, in order to initiate the proceedings and adjudicate the offences concerning computer as referred to in Chapter -9, constitute a three member Information Technology Tribunal consisting of one member each of law, Information Technology and Commerce by notification in the Nepal Gazette from amongst the persons who are qualified under section 60.

(2) The Law Member shall be the chairperson of the Tribunal.

(3) The Tribunal shall exercise its jurisdiction as prescribed.

(4) Any person aggrieved by an order or a decision made by Tribunal may appeal to the Appellate Tribunal within thirty five days from the date of such order or decision, as the case may be.

61. **Qualification of the Member of the Tribunal:** (1) Any person who has the knowledge in information technology and, who is or who has been or who

is qualified to be a judge in the District Court, shall be eligible to be a law member of the Tribunal.

(2) A Nepalese citizen who holds at least master degree in computer science or information technology and who has at least three years experience in the field of electronic transactions, information technology or electronic communication, shall be eligible to be a information technology member of the Tribunal.

(3) A Nepali citizen who holds at least master degree in management or commerce and who has specialization in the field of electronic transaction and who has at least three years experience in the related field shall be eligible to be a commerce member of the Tribunal.

62. Terms of office, remuneration and conditions of service of the Member of Tribunal: (1) The term of office of a member of the Tribunal shall be of five years and he/she shall be eligible for reappointment.

(2) Remuneration and the terms and conditions of the service of a Member of the Tribunal shall as prescribed.

(3) Every Member of the Tribunal shall, before assuming his/her office, take the oath of his/her office and secrecy before the Chief Judge of Appellate Court in a format and in a manner as prescribed.

63. Circumstances under which office shall be fallen vacant and filling up of vacancy: (1) Office of a Member of the Tribunal shall be fallen vacant in the following circumstances:

a) On expiry of terms of office,

b) On attainment of sixty three years of age.

c) On death,

d) If one tenders resignation,

e) If one is convicted by a court on any criminal offence involving moral turpitude, or

f) If it is proved that one has misbehavior or has become incompetent to perform one's duty while making an inquiry by Government of Nepal on the charge that one has misbehavior against one's office or has become incompetent to perform one's duty.

Provided that, a Member of the Tribunal charged under this Clause shall given a reasonable opportunity to defense his/her case.

(2) Notwithstanding anything contained in Clause (f), if the law member of the Tribunal is a sitting judge, while making such an inquiry, it shall be done in accordance with the prevailing law concerning his/her terms of service.

(3) The procedure of inquiry, for the purpose of Clause (f) of Sub-section Sub-section (1), shall be as prescribed.

(4) Government of Nepal shall, in case of vacancy of the office of any member of Tribunal under Sub-section (1), fulfill such vacancy from among the persons who are qualified under section 61 for remaining term of office of such a member.

64. Staff of the Tribunal: (1) Government of Nepal shall make available necessary staff to the Tribunal to perform its functions.

(2) Other provisions regarding the staff of the Tribunal shall be as prescribed.

65. Procedures to be followed by the Tribunal: The Tribunal shall, while initiating proceedings and adjudicating the case under section 60, shall follow the procedures as prescribed.

Chapter-11

Provisions Relating to Information Technology Appellate Tribunal

66. Establishment and formation of the Appellate Tribunal: (1) Government of Nepal shall, in order to hear the appeal against the order or the

decision made by the Tribunal and to hear the appeal against the decision or order made by the Controller or by the Certifying Authority, as the case may be, under this Act, by notification in the Nepal Gazette, establish a three member Information Technology Appellate Tribunal consisting of one member each of law, information technology and commerce from among the persons who are qualified under section 67,

(2) Law Member shall be the chairperson of the Appellate Tribunal.

(3) Exercise of the jurisdiction of Appellate Tribunal shall be as prescribed.

67. **Qualification of the Member of Appellate Tribunal:** (1) A person who has the knowledge in information technology and who is or who has already been or who is qualified to be a judge in the Appellate Court shall be eligible to be a law member of the Appellate Tribunal.

(2) A Nepali citizen who holds at least master degree in computer science or information technology and who has at least five years experience in the electronic transaction, information technology or electronic communication shall be eligible to be an information technology member of the Tribunal.

(3) A Nepali citizen who holds at least master degree in management or commerce and who has specialization in the field of electronic transactions and who has at least five years experience in the relevant field, shall be eligible to be a commerce member.

68. **Terms of Office, Remuneration and Terms & Conditions of the service of the Member of Appellate Tribunal:** (1) The term of office of the member of the Appellate Tribunal shall be of five years and he/she shall be eligible for reappointment.

(2) Remuneration and other terms and conditions of the services of the members of the Appellate Tribunal shall as prescribed.

(3) A member of the Appellate Tribunal shall, before assuming his/her office after appointment, take the oath of his/her office and secrecy before the Chief Justice of the Supreme Court.

69. **Conditions of Vacancy of Office and filling up of such Vacancy**: (1) Office of a Member of Appellate Tribunal shall be fallen vacant in the following circumstances:

(a) On expiry of terms of office,

(b) On attainment of sixty three years age,

(c) On death,

(d) If one tenders resignation

(e) If one is convicted by a court on any criminal offence involving moral turpitude, and,

(f) If it is proved that one has misbehavior or has become incompetent to perform one's duty, while making an inquiry by Government of Nepal on the charge that one has misbehavior against one's office or has become incompetent to perform one's duty.

Provided that, a member of the Appellate Tribunal charged under this Clause shall be given a reasonable opportunity to defense his/her case.

(2) Notwithstanding anything contained in Clause (f), if the law member of the Tribunal is a sitting judge, while making such an inquiry, it shall be done in accordance with the prevailing law concerning his/her terms of service.

(3) The procedure of inquiry, for the purpose of Clause (f) of Sub-section (1), shall as prescribed.

(4) Government of Nepal shall, in case of vacancy of the office of any member of Tribunal under Sub-section (1), fulfill such vacancy from

amongst the persons who are qualified under section 67 for remaining term of office of such a member.

70. Staff of the Appellate Tribunal: (1) Government of Nepal shall make available necessary staff to Appellate Tribunal to perform its functions.

(2) Other provisions regarding the staff of the Appellate Tribunal shall be as prescribed.

71. Procedures to be followed by the Appellate Tribunal: The Tribunal shall, while initiating proceedings and adjudicating the appeal filed before it, shall follow the procedures as prescribed.

Chapter-12

Miscellaneous

72. Provision may be made by an Agreement: The parties involved to the work for creating, transmitting, receiving, storage or for processing through any other means, of any electronic record may make the provision by an agreement, not to apply any or all provisions of the Chapter 3 or to alter some of the provisions referred to in the said Chapter in course of their business and may make the provisions to regulate their activities accordingly.

73. Government of Nepal may issue Directives: Government of Nepal may, in regard to the implementation of this Act, issue necessary directives to the Controller or Certifying Authority, and in such a case, it shall be a duty of the Controller or Certifying Authority, as the case may be, to comply with such directives.

74. Time Limitation to file a Complaint: If a violation of this Act or Rules framed hereunder has been occurred or if any act deemed to be an offence under this Act has been committed, first information report in regard to such a violation or an offence shall have to file within thirty five days of the information on which such a violation has been occurred or an offence has been committed.

75. **Government of Nepal to be a Plaintiff:** (1) Any case deemed to be an offence under this Act shall be initiated by Government of Nepal as plaintiff and such a case shall be deemed have been included in Schedule 1 of the Government Cases Act, 1992 (2049).

(2) While conducting investigation of a case under Sub-section (1), the police has to take assistance of the Controller or other concerned expert, as the case may be.

76. **Compensation to be Recovered:** If any loss or damage has been caused to any person by the reason of offence committed under this Act, the compensation of such loss or damage shall also be recovered from the offender.

77. **This Act shall not Apply**: (1) Notwithstanding anything contained elsewhere in this Act, this Act shall not be applied in the following matters:

(a) Negotiable Instruments as referred to in the Negotiable Instruments Act, 2034 (1977).

(b) Deed of will, deed of mortgage, bond, deed of conveyance, partition or any such deed related with transfer of the title in any immovable property,

(c) Any other document which demonstrates title or ownership in any immovable property,

(d) Power of Attorney, statement of claim, statement of defense or any such other documents as may be used in courts proceedings,

(e) Statement of claim, counter-claim, statement of defense or any such other document as may be submitted in writing in the proceedings of any Arbitration,

(f) Documents as prescribed by the prevailing law that requires not to retain in electronic form.

(2) Notwithstanding anything contained in Sub-section (1) Government of Nepal may, by notification in the Nepal Gazette, alter the documents referred to in Sub-section (1).

78. **Power to Frame Rules:** Government of Nepal may in order to fulfill the objective of this Act, frame necessary Rules.

79. **To Frame and Enforce the Directives:** Government of Nepal may, in order to achieve the objective of this Act, frame and enforce necessary directives, subject to this Act and Rules framed hereunder.

80. **Effect of inoperativeness of The Electronic Transactions Ordinance, 2063 (2008):** With the Electronic Transactions Ordinance, 2063 (2008) being inoperative, unless a different intention appears, the inoperativeness shall not,

(a) Revive anything not prevailing or existing at the time, at which the Ordinance became inoperative,

(b) Affect the matter in operation as per the Ordinance or anything duly done or any punishment suffered there under,

(c) Affect any right, privilege, obligation or liability acquired, accrued or incurred under the Ordinance,

(d) Affect any penalty, punishment or forfeiture incurred under the Ordinance,

(e) Affect any action or remedy made or taken in respect of any such right, privilege, obligation, liability, penalty or punishment as aforesaid; and any such legal proceeding or remedy may be instituted, continued or enforced as if the Ordinance were in force.