(Draft 5 dated 23-1-2005)
(Documents used for 8th section meeting of the Committee of Science, Technology and Environment)

LAW ON E-TRANSACTIONS

Pursuant to the Constitutions of the Socialist Republic of Vietnam of 1992 as amended by Resolution 51/2001/QH10 of 25/11/2001 of the 10th Legislature, Session No. 10;

This Law provides for e-transactions.

CHAPTER I
GENERAL PROVISION

Article 1- Governing Scope

I. Option 1 of Article 1

1. This Law governs data message; e-signatures; e-certification; e-contracting; e-transactions in Government agencies; confidentiality security and safety in e-transactions**;** protection of IPR in e-transactions, in respect of transactions related to civil, business, trading and State administrative sectors and other sectors as provided by the laws.

2. Provisions in section 1 Chapter II and Chapter III of this Law do not apply to e-transactions in the following areas:

a) Wills, inheritance;

b) Immovable assets;

c) Personal rights;

d) Commercial papers and other valuable papers;

dd) Other ***cases*** as provided for by the laws.

II. Option 2 of Article 1

1. This Law provides provisions on e-transactions activities in relation to transactions in civil, commercial, State administrative sectors and other sectors as provided by the laws.

2. Provisions on the validity of data message in Section I, Chapter II and provisions on validity of electronic signatures in Chapter II of this Law shall not apply to the following cases:

a) Wills, inheritance;

b) Immovable assets;

c) Personal rights;

d) Commercial papers and other valuable papers;

dd) Other cases as provided for by the laws.

Article 2. Scope of Application

1. This Law shall apply to domestic and foreign organizations and individuals conducting e-transactions in the territory of the Socialist Republic of Vietnam.

2. This Law shall also apply to e-transactions with foreign elements if the parties agree to choose this law as governing law or the foreign law or international treaties requires so. The parties may also agree to apply foreign laws if such [foreign] laws do not contrary to the basic principles of Vietnamese laws.

Article 3. Application of international treaties, other legal documents

1. In case where other legal documents contain provisions contrary to this Law, this Law shall apply.

2. In case where international treaties, which Vietnam has concluded or acceded to, contain provisions different to provisions of this Law, the provisions of the international treaties shall apply.

Article 4. Definition

In this Law, the following terms are defined as follows:

1. *An e- transaction* is a transaction that uses electronic means.

2. *An automatic e-transaction is a transaction that is automatically guided or conducted in part or in whole through electronic means by computer programs*.

3. *An e-contract* is a contract used electronic means in part or in whole of the process of entering into and implementation of [the contract].

4. A e-signature program is a computer program is established to independently operate or [operate] with other means, information systems, computer programs in order to create an unique e-signature for a specified person.

5**.** *An e-signature is a sign in the form of words, letters, sounds or other forms crated by an electronic means attached with a data message in order to identify the person who sign such message data*.

6. *An e-certificate* is a data message issued by a certification service provider, which ensures that the certified organization or individual is the sole owner of the e-signature.

7. *An e-certification activity* is an activity providing services certifying e-certificates and maintaining related documents.

8. *An electronic means* a means that operates based on electric, electronic, digital, magnetic, wireless, optical, electro-magnetic technologies or similar technologies

9. *A computer program* is a set of commands or instructions controlling computer programs used directly or indirectly in an information processing system to perform a certain task.

10. *Information* is words, numbers, pictures, sound, codes, computer programs, software, database or in other format.

11. *An information system* is a system used to create, send, receive, store or process data messages.

12. *A data message* is information created, transferred, received, stored or processed in e-transactions by using electronic means.

13. *An originator* of a data message is an organization or individual or organization or individual representing another organization or individual who creates or sends a data message before such a data message is stored, but does not include an intermediary that remits the data message.

14. *A Recipient of a data message* is the one who receives a data message from an originator, but does not include an intermediary that remits the data message.

15. *An intermediary* is an organization or individual representing other organizations and individuals sending and receiving or storing data messages or providing services related to such data messages.

16. *A Signatory* is a person or legal representative in control of the e-signing programs and use such means to verify his/her intentions in relation to the signed data message.

17. *A **C**ertification service provider* is an organization or individual that provides e-certification activities in accordance with the laws.

18. *Secured process* is a process used to verify an electronic record of a specific organization, individual and to prevent technical errors occurring in the process of exchange, storing[, which] may change the contents and format of the data message from a particular point of time.

Secured process may use algorithm or codes to verify letters or numbers, pin numbers, response and acknowledge the process or other similar security tools.

19. *Reliable system* is hardware, software of *computers* or computing processes that meet the requirements of ensuring security against outside intrusion or abuse; ensuring reliability and accuracy in operation, execution in accordance with the designed functions; closely connecting with the accepted secured process.

20. *Third Party* means any organization or individual which a network service provider does not have the right to control.

Article 5. Purposes of the Law on E-Transactions

1. To recognize the validity of *data messages*, e-signatures used in e-transactions;
2. To create legal environment to foster the application of e-transactions, to increase effectiveness of economic-social development, to foster scientific and technological application.
3. To foster administrative reform, integration into the international economy, to ensure security, national defense.
4. To protect lawful rights and benefits of organizations, individuals, interests of the State, public interests; to ensure equality and security in e-transactions.

Article 6. Principles for Using Electronic Media in Transactions

1. Organizations and individuals may use or may not use electronic means in their transactions.

2. The use of electronic means in transactions must be agreed by the parties unless otherwise provided by law.

3. No particular technology shall be considered a sole [technology] in electronic transactions.

4. Organizations and individuals who agree to use electronic means in transactions must comply with the provisions of this Law.

Article 7. State policy on Developing E-transactions

1. To give priority to the use of capital for development investment in applying science and technology, developing national information infrastructure, training human resources for information technology in order to foster the application of e-transactions in different areas of socio-economic life.

2. To encourage organizations, individuals to invest, apply e-transactions in different areas of the socio-economic life.

3. To support budgets for public administrative services in carrying out e-transactions.

Article 8. State Management on e-transactions

1. To develop strategies, plans and [to] issue policies for development, application of e-transactions in social-economic sectors, national defense, security.

2. To promulgate legal documents on e-transactions.

3. To develop and issue e-transaction standards.

4. To manage e-certification service providers.

5. To develop communication and information technologies *for* e-transactions.

6. To manage and implement international co-operations on e-transactions.

7. To inspect, check, supervise the implementation of the laws on e-transactions; to deal with breaches of the laws on e-transactions.

Article 9. State responsibilities on e-transactions

1. The Government shall uniformly [perform] the State management on e-transactions activities.

2. The Ministry of Post and Telecom shall be responsible before the Government on implementation of State management on e-transaction activities.

3. The Ministry of Science and Technology, Ministry of Finance, State Bank of Vietnam, Ministry of Police, Ministry of Culture-Information, [other] ministries, ministerial-level bodies within their functions, powers shall co-ordinate with the Ministry of Post and Telecom to implement State management on e-transaction activities.

4. People's Committees within their functions, powers shall implement State management on e-transaction activities in accordance with the de-centralization of the Government.

Article 10. Prohibited activities

1. Unauthorized access to computing resources.

2. Access to computers for the purpose of supporting and preparing illegal activities.

3. Distribution of illegal and false information.

4. Distribution of information that is inconsistent with the good traditional culture, ethics of Vietnamese.

5. Dissemination of information that affects sovereignty, independence and territorial integrity, national security and solidarity.

6. Illegal prevention or blockage of transmission of and access to data messages.

7. Unauthorized alteration, deletion, duplication, disclosure, display or transfer of a data message in part or in whole.

8. Illegal prevention or destruction of computer system or networks by alteration, deletion, transmission, dispatch, destruction of computer data.

9. Creation and dissemination of software program that trouble and prevent the operations of computer or data messages.

10. Creation of fake data messages in order to carrying out illegal activities.

11. Other illegal activities in e-transactions provided by the laws.

Chapter II
DATA MESSAGE

Section 1

Validity of Data Message

Article 11. Validity of Data Message

Data message is in accordance with provisions of this Law shall be valid.

Article 12. The Same Validity as Written Document

Where the law requires information to be in writing, a data message shall be the same validity as a written document if the information contained therein is accessible so as to be usable for subsequent reference.

Article 13. Validity of Original Copy

1. Where the law requires information to be presented or retained in its original form, a data message shall be considered as an original copy if:

a) There is assurance as to the integrity of the information since its first origination;

b) The contents of the data message are accessible and can be usable in its entirety for reference when necessary.

2. A data message is considered complete and intact when its contents have remain unchanged except changes in its appearance that arise in the normal course of communication, storage and display.

3. Provisions in items 1 and 2 of this Article shall apply in case the law requires that a copy or a notarized copies to be presented or retained.

Article 14. Admissibility as Evidence

1. A data message can be used to be evidence in accordance with this Law and regulations on education.

2. The admissibility of a data message shall be determined based on the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the information was maintained; the manner in which its originator was identified, and to any other relevant factors.

Article 15. Retention

1. Where the law requires that certain information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

a) The information in the data message is accessible as and when needed;

b) The data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information of the data message;

c) Such information is retained in a way to enable the identification of the origin and destination of a data message and the date and time when it was sent or received.

2. Clause 1 shall not apply to data that is merely used for sending or receiving another data message.

Section 2

Dispatch and Receipt of Data Messages

Article 16. Dispatch of Data Messages

Unless otherwise agreed by the parties, the dispatch of a data messages is determined as follows:

1. The sender of a data message shall be responsible for the data message and for all data messages sent from the information system programmed by him/her to automatically operate.

2. The recipient may consider a data message as being sent by the sender if the sender has accepted a validating procedure for confirming that a data message is sent by the sender and the recipient has followed this procedure to receive the data message from the sender.

3. Clause 2 of this Article shall not apply from the time the recipient receives a notice from the sender that the data message is not of the sender.

4. Clauses 1 and 2 of this Article shall not apply from the time when the recipient knew that there is a technical error in transmission of the data message or [the recipient] used errors-verifying methods approved by the sender.

Article 17. Time and Place of Dispatch of Data Messages

Unless otherwise agreed, the time and place of dispatch of a data message is as follows.

1. The dispatch of a data message occurs when it enters an information system outside the control of the sender.

2. A data message is deemed to be dispatched at the place where the sender has its place of business or residence. If the sender has more than one place of business, the place of business is that which has the closest relationship to the transaction had carried out or has been carrying out or, where there is no underlying transaction, the principal place of business.

Article 18. Receipt of Data Messages

Unless otherwise agreed by the parties, the receipt of a data messages is provided as follows:

1. The recipient of a data message is deemed to have received the data message when the data message enters his/her information system as provided in Article 17 of this Law.

2. The recipient is entitled to consider each data message as independent and act on it in accordance with this article unless the data are a copy of another data message.

3. Upon receipt of the data message, the recipient has to inform the sender in accordance with the method agreed by the parties according to the following order: .

a) The recipient shall inform, acknowledge the dispatch of the data message to indicate this to the sender.

b) Where the sender has stated before or during the dispatch of data that the data is conditional on receipt of the acknowledgement, the data is treated as though it has never been sent, until the acknowledgement is received by the sender through the report of the recipient acknowledging that [the recipient] has received such data message.

c) In case the sender has not stated of acknowledgement and the acknowledgement has not been received within the time specified or agreed, the sender may give notice to the recipient stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received. If the acknowledgement is not received within the time specified, the sender may treat the data message as though it had never been sent.

Article 19. Time and Place of Receipt of Data Messages

Unless otherwise agreed by the parties, the time and place of receipt of a data message are provided as follows.

1. If the recipient has designated an information system for the purpose of receiving data messages, receipt occurs at the time when the data message enters the designated information system or at the time when the data message is retrieved by the recipient. If the recipient has not designated an information system, receipt occurs when the data message enters any information system of the recipient.

2. A data message is deemed to be received at the place where the recipient has its place of business or residence unless otherwise agreed by the parties. If the recipient has more than one place of business, the place of business is that which has the closest relationship to the transaction had carried out or has been carrying out in accordance with the laws or where there is no underlying transaction, the principal place of business.

Article 20. Automatic Dispatch and Receipt of Data Messages

If the sender or the recipient has designated one or several information systems for the purpose of automatic dispatch or receipt of data messages, the provisions of Articles 16, 17, 18 and 19 of this Law shall apply.

Section 3
Secured Data Messages

Article 21. Secured Data Messages

1. Secured data messages are the ones that meet the following conditions:

a) The contents and format of data messages shall not be changed during transmission, reception or storage since a specific time;

b) It is possible to identify the sender of the message.

2. If a data message is verified to meet the conditions specified in Clause 1 of this Article, it is considered a secured message.

3. The parties may agree on procedures for verifying that a data message is secured. If the parties do not have any agreement on procedures for verification, then a reasonable verification method could be used. The reasonableness of procedures for verification is determined based on:

a) Nature of the relevant transaction;

b) Professionalism of the parties;

c) The number of similar transactions undertaken by the parties;

d) Procedures for varification of similar transactions by the parties.

4. A data message with a certified e-signature is a secured data message.

CHAPTER III

E-SIGNATURES AND CERTIFICATION OF E-SIGNATURES

Section 1

E-signatures

Article 22. Validity of e-signatures

1. E-signatures shall have same validity as normal signatures if [e-signatures] are in accordance with this Law and other related laws.

2. Where the law requires a written document to have a signature of a person, a data message is taken to have been met this requirement if satisfied the following criteria:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable and appropriate for the purpose for which the data message was generated and communicated.

Article 23. Secured E-signatures

1. Secured e-signatures are those originated with a secured process which is agreed by the parties and meet the following conditions:

a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

d) Any alteration made to that information after the time of signing is detectable.

2.The Government shall provide for detailed regulations on secured e-signatures.

Article 24. Responsibility of the Signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall have the following responsibilities:
   (a) Have means to avoid unauthorized use of its signature creation data;
   (b) Without undue delay, notify any person who rely on the e-signature and Certification Service Providers when the signatory discovers that the signature creation data may not be under the signatory's control;
   (c) Where a e-certificate is used, must apply necessary methods to ensure the accuracy and integrity of information included in the e-certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of set forth in Clause 1 of this Article.

Article 25: Responsibilities of the Party relying on e-signatures

A party relying on e-signatures shall have the responsibilities:

1. To take necessary steps to verify the reliability of an electronic signature;

2. To take reasonable steps to verify the validity of e-certificates or any limitation with respect to the certificate before accepting the e-signature.

Article 26. E-certificates and e-signatures with foreign element

1. The Government recognizes the validity of e-certificates and e-signatures with foreign element if such e-signatures or e-certificate meet the provisions on reliability in this Law.

2. The Government provides for detailed regulations on e-signatures and e-certificates with foreign elements.

Section 2

E-certification Services

Article 27. Contents of E-certification Services

1. Issuance, renewal, suspension and revocation of e-certificates.
2. Provision of necessary information to certify e-signatures of a person who sign a data message.
3. Provisions of other serivces related to e-signatures and e-certificates.
4. Other tasks as provided for by law.

Article 28. Contents of E-certificates

1. Providing accurate information about the Certification Service Provider [which issuesan e-certificate].
2. Ensuring that the owner of the e-certificate control the signature creation data at the time of issuance of the certificate and the signature creation data is valid before or at the time of issuance of the certificate.
3. Clearly identifying restrictions on the purpose or use of the certificate.
4. Clearly identifying restriction on the legal liabilities of the Certification Service Provider.

Article 29. Rights and Obligations of e-certification service providers

1. E- certification service providers shall have the following rights and obligations:

a) Carry out the tasks specified in Article 27 of this Law;

b) Comply with legislation on the establishment, organization and operations of this type of services;

c) Use reliable equipment, procedures and resources in conducting their business;

d) Assurance of the accuracy and integrity of basic data in the e-certificates issued by themselves;

dd) Publishing information related to e-certificates issued, renewed, suspended, restored or revoked;

e) Providing appropriate facilities to enable those who rely on an e-signature and competent authorities to rely on the e-certificate to ascertain the origin of a data message and e-signature;

f) Inform related parties of any failure that affects the certification of e-signatures;

h) Other obligations as provided by law.

2. The Government shall provide for detailed regulations on rights and obligations of e-certification service providers in line with Clause 1 of this Article.

Section 3

Administration of E-certification Services

Article 30: Conditions for Providing E-certification Services

1. All Vietnamese organizations and individuals may provide e-certification services if they comply with regulations on e-certification.

2. All foreign organizations and individuals may provide e-certification services if [they] meet regulations on e-certification and are licensed by the competent authority.

3. The Government shall provide for detailed regulations and conditions for providing e-certification services stipulated in this Article, including:

a). Organizational structure, function and duties, rights of e-certification service providers.

b). Provisions on issuance, renewal, suspension, restoration and revocation of the license of a e-certification service provider.

c) Technical standards, procedures, human resources and other conditions necessary for providing e-certification services by a e-certification service provider.

d) Provisions on contents and form of e-certificates.

dd) Provisions on issuance, renewal, suspension, restoration and revocation of e-certificates.

e) Provisions on storage and publication of information related to e-certificates issued by e-certification service providers.

g) Provisions on fees charged by e-certification service providers when issuing an e-certifcate and providing e-certification services.

h) Provisions on conditions and standards for a foreign certification service provider to provide e-certification services in Vietnam.

i.) Other related provisions

Article 31: State management of E-certification Services

1. Promulgation legal documents on e-certification services;

2. Promulgation regulations on e-certification services; monitoring, inspection of implementation of such regulations;

3. Promulgation and monitoring the compliance of technical standards of e-signatures, e-certificates and e-certification activities;

4. Issuance, renewal, suspension, restoration and revocation of licenses for e-certification activities of e-certification service providers in Vietnam.

CHAPTER IV
E-CONTRACTS

Article 32. Principles of entering into, execution of e-contracts

1. Parties to a e-contract shall comply with regulations on contracts and this Law.

2. When entering into, executing e-contracts, the parties shall have right to agree on technical requirements, information contents, conditions ensuring the integrity, confidentiality, certification related to such e-contracts.

3. The State shall recognize the validities of e-contracts.

4. In case where there are differences between provisions on entering into and executing e-contracts of other related regulations and provisions of this Law, the provisions of this Law shall apply.

Article 33. Validity of a Notice in E-contracts

In execution of a e-contract, a notice in the form of a data message shall be legally valid and enforceable as a notice in other traditional form.

CHAPTER V
E-TRANSACTIONS IN STATE AGENCIES

Article 34. Types of E-transactions in State Agencies

1. Types of e-transactions in State agencies include:

a) E-transactions within an agency;

b) E-transactions among different State agencies;

c) E-transactions between State agencies with organizations and individuals in accordance with law.

2. E-transactions of State agencies shall be in accordance with provisions of this Laws and other related regulations.

3. State agencies within its duties and powers shall have right to actively carry out a part or all of its transactions with organizations and individuals using electronic means and shall have responsibility for establishment of reasonable roadmaps for conducting e-transactions.

Article 35. Principles for Conducting E-transactions in State Agencies

1. When conducting e-transaction, State agencies shall determine the following:

a.) Formats, forms of data messages;

b) In case e-transactions require e-signatures, descriptions of types of e-signatures and e-certification;

c) Procedures to ensure the integrity, security and confidentiality of e-transactions;

2. A State agency can provide public services in electronic forms based on regulations of such agency. Such regulations shall not be contrary to provisions of the current laws and this Law.

Article 36. Security, confidentiality and storage of electronic information in State agencies

1. State agencies shall ensure confidentiality, security and storage of information in conducting e-transactions in accordance with the provisions of this Law and related legislation.

2. State agencies shall have [following] responsibilities when conducting e-transactions:

a). Periodic review and ensuring security of their electronic data system in conducting e-transactions.

b). Ensuring confidentiality of information related to e-transactions; not be used for other purposes; nor be closed to a third party in accordance with law on confidentiality.

c). Ensuring the integrity of data messages in e-transactions; ensuring safety in operating their computer network;

d). Creating database of corresponding transactions, ensuring information security and having standby system to recover information in case of errors of the electronic information system.

Article 37. Responsibilities of State Agencies in case of Errors of E-information System

In case e-information system of a State agency has errors, which do not ensure the safety of data messages, the agency shall be responsible for informing users immediately of the errors and taking all necessary steps to correct the errors.

Article 38. Responsibilities of Organizations and Individuals in E-transactions with State Agencies

Organizations and individuals in their e-transactions with State agencies shall comply with the regulations on e-transactions issued by the competent authority and other related laws.

Article 39. Acceptance of Electronic Forms and Electronic Information

Applications, licenses, registration, administrative documents, payment receipts, notices or other information of organization, individuals in the form of electronic shall be accepted by State authority if [these documents] satisfy provisions of Articles 34 and 35 of this Law.

CHAPTER VI

CONFIDENTIALITY, SECURITY AND SAFETY IN E-TRANSACTIONS

Article 40. Security and Safety in E-transactions

1. Organizations and individuals may exercise confidentiality measures in conducting e-transactions.

2. Organizations and individuals conducting e-transactions must take necessary measures to ensure smooth operations of the information system under their control used in e-transactions. If technical errors of the information systems cause damage to other organizations and individuals, [the organizations and individuals] shall have to pay compensation in accordance with laws.

3. Organizations and individuals shall not take any action that prevent or cause damage to normal operations of the information systems used in e-transactions unless otherwise provided for by law.

Article 41. Protection of Electronic Data

Organizations, individuals are not allowed to take any action that affects the integrity of data messages of other organizations and individuals without their agreement unless otherwise provided by law.

Article 42. Information Confidentiality

Organizations, individuals are not allowed to provide or disclose part or all of information related to private and personal affairs or information of other individuals and organizations which is accessible by or under the control [of the first-mentioned organizations and individuals] without prior agreement [of the other organizations and individuals], unless otherwise provided by law.

Article 43. Responsibility of Network Provider

1. Network providers shall be responsible for co-coordinating with relevant agencies to develop management mechanism and technical measures to prevent the use of [their] network services to disseminate data messages which are against the good traditional culture, national ethics, [and] cause harm to the national security, public order or [are] breaches of other laws and regulations .

2. Network providers shall be responsible for any data messages that are prohibited from circulation but is disseminated using the network provided by the providers if they do not comply with Clause1 of this Article.

Article 44. Responsibilities of organizations, individuals upon requests of competent State agencies

1. Upon requests of competent State agencies in accordance with the laws, organizations and individuals shall implement the following requests:

a. Storage of a particular data message including the transfer of the data message to another computer system or other storage place.

b. Maintenance of the integrity of a particular data messages.

c. Production of or providing a particular data messages they have or under their control including password and other encryption methods.

d. Presentation of or providing information related to the user of the services when the organizations and individuals being requested are computing service providers controlling this information.

dd. Other responsibilities provided by law.

2. Competent bodies and persons shall be responsible before the laws for their requests.

Article 45. Authority of State agencies

1. In accordance with the laws, competent State authority shall have the following rights:

a. search or otherwise access part or all of the computer system and data messages in such system;

b. Seize part or all of the computer system;

c. Copy and store copies of data messages;

d. Prevent access to a computer system;

e. Other rights provided by law.

2. When exercising the rights stipulated in Clause 1 of this Article, competent authorities and persons shall be responsible before the laws for their decisions.

CHAPTER VII

PROTECTION OF INTELLECTUAL PROPERTY IN E-TRANSACTIONS

Article 52. Compliance with IP Legislation in E-transactions

Intellectual property (IP) in e-transaction is subject to this Law and other IP legislation.

Article 53 – Rights and Obligations of Originators of Data Messages

1. Intellectual property rights (IPR) of subjects in data messages of an originator are protected by IP legislation.

2. The originator of a data message shall be responsible for any legal consequence of his/her action of originating and sending a data message giving rise to the following IP relations:

a) Use of industrial property objects in the data message for the purpose of selling, offering, advertising the supply of goods or services bearing IP objects that are protected in Vietnam and the remittance of the data message has real commercial impact in Vietnam;

b) Distribution of work to the public in the form of a data message containing the work whose copyright is protected in Vietnam to a networked server accessible by the public.

c) Duplication of work in the form of sending a data message containing the work whose copyright is protected.

3. The originator of a data message shall bear all legal responsibilities for actions of unfair competition stipulated in Article 50 of this Law.

Article 48 – Responsibilities of the Recipient of Data Messages

The recipient of a data message shall be all legal responsibilities for any consequence of its action of receiving the data message that gives rise to IP relations, including copying of work whose copyright is protected by printing from the computer network data messages containing this work.

Article 49 – Responsibilities of the Intermediary

1. Unless otherwise agreed by the originator and the intermediary, the intermediary when sending, receiving and storing a data message or providing a service related to the data message shall take reasonable and necessary measures to ensure the contents of the data message which has trade secret are not accessible by nor easily disclosed to people other than the recipient designated in the data message.

2. If the failure of the intermediary to comply or fully fulfill the provisions of Clause 1 of this Article leads to the disclosure of a trade secret, this shall be deemed as the action of disclosing a trade secret.

3. The intermediary shall not bear any legal responsibility for materials of a third party in the form of electronic record to which it only provides access to the materials, provided that the responsibility arises from:

a) Creation, publication and distribution of the materials; or

b) Any infringements of any right to the materials or related to the materials.

4. Clauses1, 2 and 3 of this Article shall not affect:

a) any obligation of the intermediary arising out of a contract or law;

b) Any obligations of the intermediary as provided by law or valid verdicts and decisions of the courts in respect of deletion, prevention or refusal of access to the materials.

Article 50. Prohibited Activities related to Intellectual Property in E-transactions

1. Registration of domain names which are identical or confusingly similar to trademarks, trade names, appellations of origin, and geographic indications which are protected and the persons who register the domain names are not the legal right holder of the names and marks in order to sell, lease or transfer to the right holders of the trademarks, trade names, appellations of origin, and geographic indications or competitors of these persons or prevent the right holders of the trademarks, trade names, appellations of origin, and geographic indications from registering the domain names.

2. Registration, occupation of domain names or right to domain names that are identical or confusingly similar to a protected trademark or trade name which belong to another person for the purpose of occupying and abusing the domain names or damaging the reputation of the holders of the trademark or trade name.

3. Using his/her website key words for searching which is identical with a protected trademarks, trade names of another person for the purpose of abusing the reputation of the trademarks or trade names to attract web surfers to his/her website when web surfers use the trademarks or trade names to search for the products or services of the right holders.

4. Other prohibited activities provided for by industrial property legislation.

Article 51. Responsibility of Network Service Providers in Respect of IP

1. Network service providers shall be responsible for taking necessary confidential protection measures to ensure trade secrets of the network users who want to keep confidential when uploading [these] on the network which shall not be accessible by or easily disclosed to others.

2. Network service providers shall not bear any legal responsibility for any material of a third party in the form of electronic records which they only provide access to the data, if the responsibility arises from:

a) Creation, publication and dissemination of materials;

b) Infringement of any right of the materials or related materials.

3. The provisions of Clauses1 and 2 of this Article shall not affect:

a) any obligation of a network service provider arising out of a contract or law;

b) Any obligations of a network service provider as provided by law or valid verdicts and decision of the courts in respect of deletion, prevention or refusal of access to the materials.

CHAPTER VIII
INSPECTION, DISPUTE SETTLEMENT AND HANDLING BREACHES

Article 52. Inspection of E-transactions

1. Inspection of e-transactions shall have the responsibilities for inspecting the implementation of e-transactions regulations; discovering, preventing and handling within its authorities ; ; recommending measures to enforce the regulations one-transactions.

2. Organization, duties and authority of e-transaction inspectors shall follow the provision of the regulations on Inspection.

3. The Government shall provide for organization, duties, authority and delegation of inspection in e-transactions in each area to officials of branches, localities.

Article 53. Handling of Deputes in E-transactions

Disputes in e-transactions shall be handled in accordance with law.

Article 54. Principles of handling IP disputes in e-transactions

1. The right to request, authority, order, procedures of handling breaches, disputes on IP stipulated in this Law shall be implemented in accordance with the laws on handling breaches, resolving disputes on IP.

2. Regarding breaches stipulated in provisions of Articles 55. 56 and 57 of this Law, the disputes on domain names shall be proceeded as following:

a) Regarding high-level domain names [being] national codes of Vietnam, disputes on domain names shall be handled in accordance with Vietnamese regulations on resolving disputes on domain names;

b) Regarding common high-level domain names, disputes on domain names shall be handled in accordance with regulations on resolving disputes on domain names of The Organization managing world domain name and network number.

Article 55. Responsibility for Violation of Laws in E-transactions

1. Organizations, individuals that violate laws in e-transactions, depending on the nature and seriousness of the violation, shall be subject to discipline, administrative fines and criminal prosecution; any damage caused shall be compensated as provided for by law.

2. Certification bodies, organizations, Certification Service Providers shall be suspended their operations or subject to punishments as provided for by law when they commit:

a) serious violation in e-certification activities;

b) serious violation in issuing certificates and violation of security measures to protect security, confidentiality of data messages;

c) failure to fulfill their responsibilities and obligations resulting in damage for the State and citizens;

d) Serious violation of other provisions of this Law.

3. The Government shall provide for detailed implementation guidelines on administrative sanctions and fines for administrative violations in e-transactions.

Article 56. Handling of Violation of Certification Agencies, Certification Service Providers

1. Certification agencies and certification service providers who commit the following violations shall be subject to suspension of operation, administrative sanctions provided for by law depending on the nature and seriousness of the violations:

a) Operations not in line with law;

b) Failure to obtain a business registration, provision of services that are not in their registered business lines or not authorized by the competent State authority;

c) Failure to fulfill required duties ;

d) Serious violations of other provisions of this Law.

2. Certification service providers shall have to suspend their operations or subject to penalty in accordance with the laws if they do not have a decision on establishment.

Article 57. Handling of Violations by Individuals

Individuals who commit the following violations shall be subject to discipline, administrative sanctions or criminal prosecution provided for by law depending on the nature and seriousness of the violations; any damage caused shall be compensated as provided for by law:

1. Failure to act within its authorized duties, authorization or wrongfully decide resulting in damage for the State, bodies, organization and citizens;

2. Failure to comply with regulations on storage and confidentiality as provided for by law.

3. Interference into the work of certification service providers without authorization by laws;

4. Violations of provisions and prohibited actions of this Law.

CHAPTER IX
IMPLEMENTING PROVISIONS

Article 58. Application of e-transactions in political, political-social organizations

Based on provisions of this Law and other related regulations, political and political-social organizations provides for the application of e-transactions within its organization.

Article 59. Effectiveness

This Law shall take effect on ....,2006.

Article 60. Implementing Regulations

The Government shall provide for detail regulations and implementation guidelines of this Law.

This Law is passed by XI National Assembly, section no. … dated….

Chairman of the National Assembly

Nguyen Van An