# Draft Law by Akram Sheikh 2014

An Act to consolidate laws relating to electronic documents and cybercrimes.

WHEREAS it is expedient to provide for legal facilitation of electronic documents and prevention of cybercrimes;
WHEREAS it is expedient to recognize, prevent and suppress cybercrimes committed by means of electronic devices through specialist mechanisms of investigation, prosecution and trial of such cybercrimes;
AND WHEREAS it is expedient to facilitate, enable and support documents, communications, transactions, information, and commerce carried out by means of electronic devices;

CHAPTER I - SHORT TITLE. EXTENT AND COMMENCEMENT

1. Short title, **extent and commencement:** (1) This Act may be called the Electronic Documents and Prevention of Cybercrimes Act, 2014.
(2) It extends to the whole of Pakistan.
(3) It shall come into force at once.

2. **Definitions**: (1) In this Act, unless there is anything repugnant in the subject or context:
(a) "access" in its variations means gaining entry into, instructing or communicating with any electronic device;
(b) "accreditation certificate" means a certificate granted by the Cyber Authority to a certification service provider;
(c) "accreditation certification service provider" means a certification service provider accredited under this Act to issue certificates for the use of its cryptography services;
(d) "addressee" means the person intended by the originator to receive the electronic document but does not include an intermediary;
(e) "affixing electronic signature" in its variations means usage of any method or process for the purpose of authenticating an electronic record, document or data by means of an electronic signature;
(f) "authenticity" means, in relation to an electronic document or electronic signature, the identification of and attribution to a particular person or information system;
(g) "Authority" means the Cyber Authority of Pakistan established under Section 21;
(h) "automated" means without human intervention using an electronic device;
(i) "certificate" means a certificate issued by a certification service provider for the purpose of confirming the authenticity or integrity or both, of the information contained therein, of an electronic document or of an electronic signature in respect of which it is issued;
(j) "certification practice statement" means the statement prepared by a certification service provider specifying the practices it employs in relation to the issuance of certificates and matters connected therewith;
(k) "Code" means the Code of Criminal Procedure, 1898 (Act V of 1898);
(l) "computer" includes but not limited to an electronic device or information system having information processing capabilities;
(m) "computer network" means the interconnection of one or more computers through the use of any communication media including the Internet, cyberspace and the use of terminals whether or not interconnection is continuous;
(n) "cryptography services" means services in relation to the transformation of contents of an electronic document from its original form to one that cannot be understood or decoded by any unauthorized person;
(o) "cybercrime" in its variations means, but not limited to, the offences mentioned in Chapter VI of this Act and any other offence, under any other law for the time being in force, committed by means of an electronic device;
(p) "data" means representation of information or knowledge in any format which are being prepared or have been prepared for use in any electronic device;
(q) "electronic device" means electrical, digital, magnetic, optical, wireless, analogue, radio, electromagnetic, electrochemical, electromechanical or any technology having equivalent information processing capabilities and includes computer, computer network, information system and such other devices, machines and gadgets;
(r) "electronic document" in its variations includes forms, documents, records, information, communications or transactions carried out by means of electronic devices;
(s) "electronic forms" includes non-tangible means of attestation on electronic devices including books, books of accounts, certificate, charts, deed,

document, document of title, execution, instrument, ledger, map, original, plans, publish, record, register, seal, witnessing, words, writing etc.;
(t) "electronic signature" means authenticating an electronic record, document or data by means of any character or combination of any characters in electronic form and includes a digital signature;
(u) "Emergency Response Team" means the Cyber Emergency Response Team established under Section 28;
(v) "Federal Government" means the authorized officer of the Federal Government designated by President of the Islamic Republic of Pakistan
(w) "function" in relation to a computer includes logic, control, arithmetical process, deletion, storage and retrieval and communication to or within a an electronic device;
(x) "Fund" means the Cyber Authority Fund established under Section 32;
(y) "information" includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;
(z) "information system" means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information;
(aa) "Investigation Team" means the Cyber Investigation Team constituted under Section 24;
(bb) "intermediary" means a person acting as a service provider in relation to the sending, receiving, storing or processing of the electronic document or the provision of other services in relation to it;
(cc) "key pair" means a private and its mathematically related public key which are so related that the public key can verify an electronic signature created by the private key;
(dd) "network service provider" means a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services usually used with electronic devices;
(ee) "originator" means a person by whom, or on whose behalf, electronic document purports to have been generated or sent prior to receipt or storage, if any, but does not include an intermediary;
(ff) "person" includes an individual, Federal Government, trust, waqf, association, statutory body, firm, company including joint venture or consortium, or any other entity whether registered or not;

(gg) "prescribed" means prescribed by Rules made under this Act;
(hh) "private key" means the key of a key pair used to create an electronic signature;
(ii) "Prosecution Team" means the Cyber Prosecution Team constituted under Section 27;
(jj) "public key" means the key of a key pair used to verify an electronic signature and listed in the certificate
(kk) "secure system" means electronic device which is reasonably secure and reliable from unauthorized access and entry;
(11) "security procedure" means a procedure which:
(i) is agreed between parties;
(ii) is implemented in the normal course by a business and which is reasonably secure and reliable; or
(iii) in relation to a certificate issued by a certification service provider, is specified in its certification practice statement;
for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices;
(mm) "subscriber" means a person who subscribes to the services of a certification service provider;
(nn) "Tribunal" means the Cyber Tribunal established under Section 41;
**(00)** "unauthorized access" in its variations means gaining entry into, instructing or communicating with any electronic device with intent or having reasonable cause to believe that such access is not authorized or in the knowledge of the person who owns or controls such electronic device;

CHAPTER II- ELECTRONIC DOCUMENTS AND ELECTRONIC SIGNATURES

**3. Authentication of electronic documents:** (1) Any subscriber may authenticate an electronic document by affixing his electronic signature.
(2) Any person by the use of a public key of the subscriber can verify the electronic document.
(3) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

4. Electronic signature: (1) Any subscriber may authenticate an electronic document by such electronic signature, which is reliable.
(2) For the purposes of this section, an electronic signature shall be considered reliable *if:*

(a) the electronic signature was, at the time of signing, within the context in which it was used, linked to the signatory or originator and to no other person;
(b) the electronic signature was, at the time of signing, under the control of the signatory or originator and to no other person;
(c) any alteration in the electronic signature is detectable;
(d) it fulfills such other procedure as prescribed by the Cyber Authority.
(3) The Cyber Authority may prescribe the procedure for the purpose of ascertaining whether the electronic signature is that of the person by whom it is purported to have been affixed.
(4) The Cyber Authority may add or omit any electronic signature and the procedure for affixing such signature.

5. Legal recognition **of electronic documents:** (1) The requirement under any law for any document, record, information, communication or transaction to be in written form shall be deemed to have been satisfied if it is:
(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference.
(2) Electronic documents shall not be denied legal recognition, admissibility, validity, proof or enforceability on the grounds that it is in an electronic form and has not been attested by any witness.

6. Legal recognition of electronic signatures: (1) The requirement under any law for any document, record, information, communication or transaction to be authenticated by affixation of signature shall be deemed to have been satisfied if it is authenticated by means of an electronic signature affixed in such manner as prescribed by the Cyber Authority.

**7. Proof of electronic** signature: (1) An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both.

8. Presumption attached to electronic signature: (1) In any proceedings, involving an electronic signature, it shall be presumed unless evidence to

contrary is adduced, that:
(a) the electronic document affixed with an electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; or
(b) the electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time.

**9. Requirement for document to be in** original form: (1) The requirement under any law for any document, record, information, communication or transaction to be presented or retained in its original form shall be deemed satisfied by presenting or retaining the same if:
(a) there exists a reliable assurance as to the integrity thereof from the time when it was first generated in its final form; and
(b) it is required that the presentation thereof is capable of being displayed in a legible form.
(2) For the purposes of clause (a) of sub-section (1);
(a) the criterion for assessing the integrity of the document, record, information, communication or transaction is whether the same has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and
(b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information, communication or transaction was generated and all other relevant circumstances.

**10. Use of electronic documents and electronic signatures by Federal Government:** (1) The requirement under any law for the following shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the Federal Government.
(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the Federal Government in a particular manner;
(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
(c) the receipt or payment of money in a particular manner.

**11. Legal recognition of contracts formed through electronic documents:**
(1) The requirement under any law for contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals, as the case may be, to be expressed in written or verbal form shall be deemed to have been satisfied where the contract formation is expressed through the use of electronic documents and electronic devices.
(2) The Cyber Authority may prescribe the procedure for electronic contract formation and ascertaining as to whether a contract has been properly formed through the use of electronic documents and electronic devices.

12. Retention of records: (1) The requirement under any law that any particular document, record, information, communication or transaction shall be retained for any specific period, then that requirement shall be deemed to have been satisfied by retaining the same in electronic form if:
(a) the contents of the electronic document remain accessible so as to be usable for subsequent reference;
(b) the contents of the electronic document are as originally generated, sent or received, or can be demonstrated to represent accurately the contents and form in which it was originally generated, sent or received; and
(c) the details of the electronic document such as its origin, destination, date and time of dispatch or receipt is retained.
Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

13. Sections 10, 11 and 12 not to confer rights upon any person: (1) Nothing contained in Sections 10, 11 and 12 shall confer rights upon any person to insist that any office, authority, body or agency owned or controlled by the Federal Government should accept, issue, create, retain and preserve any document in electronic form.

**14.** Stamp Duty: (1) Notwithstanding anything contained in the Stamp Act, 1899 (II of 1899), for a period of four months from the date of commencement of this Act or till the time the Federal Government devise and implement appropriate measures for payment and recovery of stamp duty through electronic means, whichever is later, stamp duty shall not be payable in respect of any instrument executed in electronic form.

**15.** Attestation **and** notarization: (1) Notwithstanding anything contained in any law for the time being in force, no electronic document shall require attestation and notarization for a period of four months from the date of commencement of this Act or till the time the Federal Government devise and implement measures for attestation and notarization of electronic documents, whichever is later.

**16. Certified copies:** (1) Where any law requires or permits the production of certified copies of any records, such requirement or permission shall extend to printouts or other forms of display of electronic documents where, in addition to fulfillment of the requirements as may be specified in such law relating to certification, it is verified in the manner laid down by the Federal Government.

17. Cyber Authority **to prescribe regulations in respect of electronic signatures:** (1) The Cyber Authority may, by notification in the official gazette, prescribe regulations, for carrying out the purposes of this Act.
(2) Without generality of the foregoing, the Cyber Authority shall prescribe regulations in respect of:
(a) all matters related to electronic signatures;
(b) all matters related to certification and attestation of electronic documents;
(c) all matters related to the retention of electronic documents;
(d) all other matters related to electronic signatures and electronic documents.

CHAPTER III- ATTRIBUTION OFELECTRQNIC DOCUMENTS

18. Attribution of electronic documents: (1) Unless otherwise agreed as between an originator and the addressee, an electronic document shall be deemed to be that of the originator if it was sent:
(a) by the originator himself;
(b) by a person who had the authority to act on behalf of the originator in respect of that electronic document; or
(c) by an automated information system programed by or on behalf of the originator to operate automatically.
(2) Unless otherwise agreed as between the originator and the addressee, the addressee is to regard an electronic document as being that of the originator, and is entitled to act on that assumption if:
(a) the addressee has no reason to suspect the authenticity of the electronic document; or
(b) there do not exist any circumstances where the addressee knows, or ought to have known by exercising reasonable care, that the electronic communication was not authentic.

**19. Acknowledgment of receipt:** (1) Where the originator has stated that the electronic document is conditional on receipt of acknowledgment, the

electronic document is to be treated as though it had never been sent, until the acknowledgment is received.
(2) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by:

(a) any document, automated or otherwise, by the addressee; or
(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic document is received.

**20. Time and place of dispatch and receipt of electronic document: (1)**
Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic document occurs when it enters an electronic device outside the control of the originator.
(2) Unless otherwise agreed between the originator and the addressee, or unless proved otherwise, the time of receipt of an electronic document is determined as follows:
(a) if the addressee has designated an electronic device for the purpose of receiving the electronic document, receipt occurs:
(i) at the time when the electronic document enters the designated electronic device; or
(ii) if the electronic document is sent to an electronic device of the addressee that is not the designated electronic device, at the time when the electronic document is retrieved by the addressee;
(b) if the addressee has not designated an electronic device, receipt occurs when the electronic document enters the electronic device of the addressee.
(3) Sub-section (2) applies notwithstanding that the place where the electronic device is located may be different from the place where the electronic document will be deemed to have been received under subsection (4).
(4) Unless otherwise agreed between the originator and the addressee, an electronic document will be deemed to have been dispatched at the place where originator ordinarily resides or has his place of business, and will be deemed to have been received at the place where the addressee ordinarily resides or has his place of business.
(5) For the purpose of this section:
(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of

business;
(b) if the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence; and
(c) "usual place of residence" in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

CHAPTER IV - CYBER AUTHORITY:

**21. Establishment of the Cyber Authority:** (1) Within sixty days of the promulgation of this Act, the Federal Government shall, by notification in the official Gazette, establish a Cyber Authority of Pakistan.
(2) The Cyber Authority of Pakistan shall be a body corporate with perpetual succession and a common seal, and shall by the said name sue or be sued.
(3) The Cyber Authority of Pakistan shall comprise of seven members, with five members from the private sector and two members from the public sector. One of the members shall be designated as the Chairman by the Federal Government.
(4) The Chairman and members of the Cyber Authority shall be appointed by the Federal Government for a term of three years and shall be eligible for reappointment only once for an equal term after the expiry of their first term of appointment.
(5) The quorum of the Cyber Authority shall be four members. No act or proceeding of the Cyber Authority shall be invalid by reason only of existence of any vacancy amongst its members or any defect in its constitution discovered after such act or proceeding of the Cyber Authority.
(6) The Cyber Authority may, from time to time, delegate one or more of its functions and powers to one or more of its members.
(7) A member of the Cyber Authority shall not be removed except on the grounds of misconduct or incapacity as adjudicated by a court of competent jurisdiction.
(8) Once appointed, no member shall have any direct financial or other interest in any entity or business relating to any services to which the Cyber Authority is authorized to function or perform.
(9) Decisions of the Cyber Authority shall be taken by a majority of the members, however the Chairman shall have a casting vote in case of a tie.
(10) Save as provided herein, the terms and conditions of service of the members of the Cyber Authority shall be such as may be prescribed by the Federal Government.

(11) The Cyber Authority shall have the power to coopt any person or institution, on such terms and conditions as it may decide, to carry out the purposes of this Act and other matters connected thereto.

22. Qualifications of members: (1) Of the seven members of the Cyber Authority:
(a) four shall be professionals or academics with at least seven years work experience in the fields of information technology, internet services, telecommunications and cryptography services;
(b) two shall be advocates with at least seven years experience and adequate knowledge of laws relating to information technology, internet services, telecommunications and cryptography services;
(c) one shall have an administrative background with at least seven years experience in a private or public organization.

23. Functions of the Cyber Authority: (1) The Cyber Authority shall perform such functions as are specified in this Act or as may be prescribed by rules made by the Federal Government.
(2) Without prejudice to the generality of the foregoing, the Cyber Authority shall:
(a) ensure that cybercrimes, as provided under this Act and otherwise, are effectively prevented, suppressed, investigated and prosecuted;
(b) cooperate and coordinate with the concerned organs of the Federal Government and other non-governmental organizations in the formulation and preparation of a national cyber-security plan;
(c) organize a Cyber Investigation Team composed of members of the Cyber Authority and other persons, as may be designated by the Cyber Authority, to exclusively investigate persons involved in violations of this Act and other matters connected thereto;
(d) organize a Cyber Prosecution Team composed of members of the Cyber Authority and other persons, as may be designated by the Cyber Authority, to exclusively prosecute persons involved in violations of this Act and other matters connected thereto;
(e) organize a Cyber Emergency Response Team composed of such persons, as may be designated by the Cyber Authority, to respond to national and significant cyber security incidents as and when they occur and to reduce risks of such incidents in the future;
(f) prescribe rules and regulations to set the powers and functions of the Cyber Investigation Team and Cyber Prosecution Team;

(g) cooperate and coordinate with domestic and international persons, entities and agencies in relation to prevention, suppression, investigation or prosecution of cybercrimes and to fulfill other purposes of this Act and the matters connected thereto;
(h) facilitate international cooperation on intelligence, investigations, training and capacity building in order to prevent, suppress, investigate and prosecute cybercrimes as provided under this Act and other matters connected thereto;
(i) monitor cybercrime cases as prevented and suppressed by cooperating and participating domestic and international law enforcement agencies;
(j) cooperate and coordinate with any office, authority, body or agency owned or controlled by the Federal Government, the business community, the civil society, non-governmental entities and such other persons deemed appropriate by the Cyber Authority;
(k) collect or record by electronic means traffic data in real-time associated with specified electronic documents transmitted by means of electronic devices;
(l) direct or instruct any governmental or non-governmental entities including network service providers to cooperate and assist the Cyber Authority in fulfilling the purposes of this Act and other matters connected thereto;
(m) grant and renew accreditation certificates to certification service providers, their cryptography services and security procedures;
(n) monitor and ensure compliance by accredited certification service providers with the provisions of this Act and the terms of their accreditation and to revoke or suspend accreditation in the manner and on the grounds as may be specified in regulations by the Cyber Authority;
(o) recognize or accredit foreign certification service providers;
(p) establish and manage the repository of its documents;
(q) carry out research and studies in relation to information technology, internet services, telecommunications and cryptography services and to obtain public opinion in connection therewith;
(r) recommend and suggest to the Federal Government the enactment of appropriate laws, issuances, measures and policies;
(s) make rules and regulations to fulfill and carry out the purposes of this Act and other matters connected thereto;
(t) encourage uniformity of standards and practices;

(u) give advice and recommendations to any person, including governmental and non-governmental entities, in relation to any provision of this Act and other matters connected thereto;
(v) perform such other functions as may be prescribed by the Federal Government to fulfill the purposes of this Act and other matter connected thereto, including proper implementation of this Act and all matters related to prevention, suppression, investigation and prosecution of cybercrimes.

**24. Cyber Investigation Team:** (1) For the purpose of investigating violations of this Act, rules and regulations made hereunder, decisions of the Cyber Authority and other matters connected thereto, the Cyber Authority shall appoint from amongst the members and other persons, an Investigation Team or Teams, headed by a member of the Cyber Authority.
(2) The Investigation Team shall, after giving the person referred to in subsection (1) a reasonable opportunity of hearing and on establishing that the person has committed the contravention, may recommend imposition of penalty or award compensation in accordance with provisions of the contravened sections of this Act.
(3) The Investigation Team shall present the violation so committed under subsection (2) to the Cyber Authority, which may, through an order in writing, impose penalty or award compensation.
(4) The Investigation Team shall prepare a case for and to the Prosecution Team, disclosing the complete facts and circumstances, their findings and recommendations, and any other material relevant for the purposes of prosecution, for its proper presentation before the appropriate forum of law.

**25. Factors to be taken into account by the Investigation Team: (1) In**
determining the seriousness and extent of the crime, the Investigation Team shall have regard to the following factors:
(a) the amount of unfair gain and loss, wherever quantifiable;
(b) the repetitive nature of the act or conduct;
(c) regulations that the Cyber Authority may prescribe in this behalf.

**26. Powers of** the **Cyber Investigation Team:** (1) Subject to the regulations prescribed by the Cyber Authority, the Investigation Team shall be entitled to:
(a) access and inspect the operation of any electronic device and any data or program residing therein;
(b) access and inspect any information, code, program, technology and other tangible and non-tangible materials;

(c) require any person to explain or clarify any matter related to any electronic device whether in his ownership, control or otherwise;
(d) require any agency, body or functionary of the state or government to assist in the investigation and implementation;

**27. Cyber Prosecution Team:** (1) For the purpose of prosecuting persons violating provisions of this Act, rules made hereunder, decisions of the Cyber Authority and other matters connected thereto, the Cyber Authority shall appoint from amongst the members and other persons possessing relevant experience, a Prosecution Team or Teams headed by a member of the Cyber Authority.
(2) The Prosecution Team shall receive presentation of the case from the Investigation Team along with the complete facts and circumstances, findings and recommendations of the Investigation Team, and any other material relevant for the purposes of prosecution, for its proper presentation before the appropriate forum of law.
(3) Subject to the regulations prescribed by the Cyber Authority, the
Investigation Team shall be entitled to all the powers and procedures of the
Investigation Team.

**28. Cyber Emergency Response Team:** (1) For the purpose of responding to national and significant cyber security incidents, as and when they occur, and to reduce risks of violations of this Act and other matters connected thereto, the Federal Government shall appoint a Cyber Emergency Response Team.
(2) The Federal Government shall specify the matters in relation to which the Cyber Emergency Response Team may perform its functions.
(3) The Cyber Emergency Response Team shall consist of a Chairperson and two members.
(4) The Chairman of Cyber Emergency Response Team shall be the Secretary of the Ministry of Information Technology.
(5) The Federal Government shall appoint, in consultation with the Chairman, two members of the Cyber Emergency

Response Team possessing at least fourteen years work experience in the fields of information technology, internet services, telecommunications and cryptography services.
(6) The Cyber Emergency Response Team shall perform such functions as may be prescribed by the Federal Government.
(7) Without generality of the foregoing, the Cyber Emergency Response Team shall perform the following functions:
(a) respond and advise on national and significant cyber security incidents;

(b) develop strategies to prevent and suppress cybercrimes, violations of this Act, decisions of the Cyber Authority, rules or regulations made hereunder;
(c) analyze the trends and patterns of cyber related offences and violations provided for under this Act;
(d) suggest to the Federal Government the enactment of appropriate laws, issuances, measures and policies;

**29. Grant of** Accreditation: (1) The Cyber Authority may grant accreditation to certification service provider, its cryptography services, electronic signature and security procedures to any person who complies with the criteria and requirements specified in the regulations prescribed by the Cyber Authority.
(2) The terms and conditions of the accreditation, including those relating to duration of the accreditation, renewal, suspension, revocation, fee for grant and renewal, shall be specified in regulations prescribed by the Cyber Authority.

30. Certification Practice Statement: (1) Any person, desirous of being accredited, shall prepare and have at all times accessible a certification practice statement in such form and with such details, particulars and contents as may be specified in regulations prescribed by the Cyber authority.
(2) Subject to such limitations as may be specified in the regulations made under sub-section (1), a certification service provider shall, during the period of validity of an accreditation certificate published for reliance by any person, be deemed to warranting to such person provided that:
(a) the certification service provider has complied with the requirements of this Act, rules and regulations made under this Act; and
(b) the information contained in the certificate is accurate.
(3) The Cyber Authority may suspend or revoke the accreditation of a certification service provider for failure to comply with the provisions of this section:
Provided that, an order for suspension or revocation of accreditation shall be made in the manner specified in regulations made under sub-section (1) after providing reasonable right of hearing.

**31.** Certification Service Providers: (1) Nothing in this Act shall impede or in any way restrict the rights of any accredited certificate service provider to engage in the business of providing certification services without being accredited.

(2) No person shall hold himself out as an accredited certification service provider unless he holds a valid accreditation certificate issued by the Cyber Authority.

**32.** Establishment of Cyber Authority Fund: (1) The Cyber Authority shall, for the purposes of this Act, establish a Fund to be called Cyber Authority Fund to meet costs and charges incurred in connection with its functions and purposes as provided for under this Act.
(2) The Fund shall consist of:
(a) such sums as the Federal Government may, from time to time, grant for the purposes of meeting any of its obligations or discharging any of its functions;
(b) loans, aid, grants and donations from the national or international agencies;
(c) receipts from sale of publications, databases, other products and services provided by Cyber Authority; and
(d) all other sums or property which may in any manner become payable to or vested in the Cyber Authority in respect of any matter incidental to the exercise of its functions and purposes under this Act.

33 Expenditure: (1) The Fund shall be expended for the purposes of:
(a) paying any expenditure lawfully incurred by the Authority;
(b) paying any other expenses, costs or expenditure properly incurred or accepted by the Cyber Authority or any of its agencies including the, Cyber Investigation Team, Cyber Prosecution Team and the Cyber Emergency Response Team, in the performance of its functions or the exercise of its powers under this Act; and
(c) repaying any moneys borrowed under this Act and the profit, return, mark - up or interest due thereon howsoever called.

(2) The Cyber Authority shall, in respect of each financial year submit for approval to the Federal Government, on such date as may be prescribed, a statement of the estimated receipts and expenditure, including requirements of foreign exchange for the next financial year.

34. Investments: (1) The Cyber Authority may insofar as moneys available in the Fund, are not required to be expended under this Act, make such investments as it may determine from time to time, in accordance with policies formulated by the Federal Government.

**35. Bank accounts:** (1) The Chairman may, with the approval of the Cyber Authority, open and maintain accounts in rupees or in any foreign currency at such scheduled bank as it may from time to time determine in accordance with instructions of the Federal Government.

**36. Audit and accounts:** (1) The accounts of the Cyber Authority shall be maintained in such manner as Federal Government, in consultation with the Controller General of Accounts, determine.
(2) The Auditor-General of Pakistan shall conduct audit of the accounts of the Cyber Authority.
(3) A copy of the audit report shall be sent to the Federal Government, along with the comments of the Cyber Authority.

37. Annual report: (1) The Cyber Authority shall prepare and publish an annual report covering its performance during the financial year for submission to the Federal Government.
(2) The annual report shall include:
(a) activities of the Cyber Authority during the financial year;
(b) an outline of programs for the year ahead;
(c) a short financial statement of the preceding year;
(d) an audited balance sheet;
(e) an audited statement of income and expenditure; and
(f) any other matter which the Federal Government may direct or the Cyber Authority may consider appropriate.

38. Repository: (1) The Cyber Authority shall establish and manage a repository for all accreditation certificates, certificates issued by accredited certification service providers and for such other information or material as may be specified in regulations prescribed by the Cyber Authority.
(2) The Cyber Authority shall take appropriate measures to ensure the security of all information or material contained in the repository.
(3) All information or material contained in the repository shall be open to public inspection, subject to regulations prescribed by the Cyber Authority.
(4) Notice of suspension or revocation of any accreditation or of certificate issued by an accredited certification service provider, shall be posted in the repository within the prescribed time.

39. Decisions of the **Cyber** Authority: (1) All applications and matters coming before the Cyber Authority shall be decided through a speaking order, as expeditiously as possible but not later than ninety days except in extraordinary circumstances and for reasons to be recorded

40. Appointment of offices, employees, advisers and other persons: (1) The Cyber Authority may appoint such officers, employees, advisers and other

persons as it may consider necessary for the efficient and proper performance of its functions provided under this Act on such terms and conditions as it may prescribed by regulations made by the Cyber Authority.
(2) The Cyber Authority may establish regional or local offices as may be necessary for efficient and proper performance of its functions as provided for under this Act.

CHAPTER V - CYBER TRIBUNAL

**41. The Cyber Tribunal:** (1) The Federal Government shall, by notification, establish tribunal to be known as the Cyber Tribunal whose principal seat shall be located in Islamabad.
(2) The Federal Government shall specify the matters in relation to which the Cyber Tribunal may exercise jurisdiction.
(3) The Federal Government shall further specify the places where the Cyber Tribunal may hold its sittings.
(4) The Cyber Tribunal shall consist of a Chairperson and such number of other members as the Federal Government may deem necessary.
(5) The appointment of Chairperson and members of the Cyber Tribunal shall be made by the Federal Government in

consultation with the Ministry of Law, Justice and Parliamentary Affairs, Government of Pakistan;
(6) The Chairperson may constitute benches of the Cyber Tribunal with as many members as the chairperson may deem necessary;
(7) The Chairperson may transfer a member of the Cyber Tribunal from one bench to another bench;
(8) The Chairperson may, if it appears that the case or matter ought to be heard by a bench consisting of more members, transfer the case or matter to such bench as the Chairperson may deem appropriate;
(9) The bench of the Cyber Tribunal may exercise such jurisdiction, powers and authority as may be prescribed by the Federal Government.
(10) An appeal from any decision of the Cyber Authority or any other agencies, including the Cyber Investigation Team, Cyber Prosecution Team and the Cyber Emergency Response Team, shall lie to the Cyber Tribunal within sixty days of such decision.
(11) An appeal from any decision of the Cyber Tribunal shall lie to the High Court within sixty days of such decision.

Provided that the High Court, if on being satisfied that grounds for condoning the delay exist, may allow an appeal after the limitations stipulated under subsection (10) and (11).

**42. Qualifications of the Chairperson and members of** the **Cyber Appellate Tribunal: (1) A person** shall not be qualified for appointment as a Chairperson of the Cyber Tribunal unless he is or has been a **judge of the High** Court.
(2) A person shall not be qualified for appointment as a member unless he has for a period of not less than ten years been an Advocate of the High Court or he has for a period of not less than fourteen years been a professional in the fields of information technology, internet services, telecommunications and cryptography services.

CHAPTER VI- CYBERCRIMES AND PUNISHMENTS

43. Punishment for committing crimes against Pakistan: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in imminent and real danger to any interests of Pakistan including, but not limited to, national security, national economy or public order, shall be punishable with imprisonment of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.

44. Punishment for damage to electronic device: (1) Any person who by means of an electronic device, without permission of the owner of such electronic device or of any other person who is controller of such electronic device, performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in any of the following acts shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.
(a) To access or secure access to any electronic device.
(b) To download copies or extracts of any data or program from any electronic device including data or program held in any removable storage device.
(c) To introduce or causes to be introduced any computer related virus into any electronic device.
(d) To damage or causes to be damaged any electronic device or any other data or program residing therein.
(e) To disrupt or causes disruption of any electronic device.
(fJ To deny or causes the denial of access to any person authorized to access any electronic device or any other programs residing therein.

(g) To charge the services availed of by a person to the account of another person by tampering with or manipulating any electronic device.
(h) To destroy, delete or alter or causes any person to destroy, delete or alter any information residing in an electronic device or diminishes its value or utility or adversely affects it by any means.
(i) To steal, conceal, destroy, or alter or causes any person to steal, conceal, destroy or alter any information residing in any electronic device.
(j) To tamper or causes another to tamper any computer source code used for an electronic device, when the computer source code is required to be maintained by any law in force.

| |
|---|
| **45. Punishment for hacking:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in hacking of or otherwise gaining unauthorized access into any electronic device, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **46. Punishment for unauthorized interception:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in unauthorized access or interception of transmission, communication or data, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **47. Punishment for dishonestly receiving electronic device: (1)** Any person who dishonestly receives or retains any stolen electronic device or any information or data therein knowing or having reason to believe the same to be received or retained dishonestly, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **48. Punishment for identity theft:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in fraudulent or dishonest use of an electronic signature, password or any other unique identification feature of any other person, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **49. Punishment for personation:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in personating any other person or otherwise pretending to be any other person, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **50. Punishment for violation of privacy:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in violating any other person's privacy, in any manner whatsoever, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| **51.** Punishment for electronic fraud: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in enticement, induction or promotion of any person to enter into a fraudulent financial relationship, in order to achieve wrongful monetary gain or loss, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both. |
| 52. Punishment for cyber terrorism: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in threatening the national security of Pakistan, striking terror in any person, destruction of property or committing any other crime termed as terrorist act, shall be punishable with imprisonment of a term not exceeding seven years or fine not exceeding one million rupees, or both. |
| 53. Punishment for cyber stalking, **spamming, spoofing and** squatting:<br>(1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in harassment, intimidation, or coercion, shall commit the crime of cyber stalking.<br>(2) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in transmission of fraudulent, misleading, or unsolicited electronic messages in bulk or otherwise to any person without his express permission, shall commit the offence of cyber spamming.<br>(3) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending of electronic messages with a counterfeit source, depicting to be an authentic source, so as to gain unauthorized access or obtain valuable information in an unlawful manner, shall commit the crime of cyber spoofing.<br>(4) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in acquisition of a domain name in bad faith to mislead, defame and deprive others from registering the same, shall commit the crime of cyber squatting. |

(5) Any person who commits the offence of cyber stalking, spamming, spoofing or squatting as described in sub-sections (1), (2), (3) or (4) respectively shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.

54. Punishment for transmitting offensive messages: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any information that is offensive, obscene or false in any manner whatsoever and sent for the purpose of causing annoyance, inconvenience, intimidation, hatred, deception, insult, obstruction or injury, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.

55. Punishment for transmitting material containing sexually explicit acts: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any material which contains sexually explicit, obscene, or indecent acts or conduct, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.

56. Punishment for transmitting material depicting children in sexually explicit acts: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any material which contains a child or minor engaged in sexually explicit act or conduct, shall be punishable with imprisonment of a term not exceeding seven years or fine not exceeding one million rupees, or both.
(2) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in enticement, induction or promotion of a child or minor to enter into any unethical or immoral relationship, shall be punishable with imprisonment of a term not exceeding seven years or fine not exceeding one million rupees, or both.
Provided that for the purposes of this section, "children" and "minors" shall mean persons who have not attained the age of 18 years.

57. Punishment for transmitting material containing heinous acts: (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in sending, generating, publishing or transmitting any material which contains any act or conduct that may be considered heinous, odious and atrocious, shall be punishable with imprisonment of a term not exceeding three years or fine not exceeding five hundred thousand rupees, or both.

**58. Punishment for failure to protect data:** (1) Any person who is responsible for possessing, dealing or handling any sensitive personal data in a electronic device which it owns, controls or operates, and negligent in implementing and maintaining security practices and procedures, thereby causing wrongful loss or gain to any person, shall be liable to pay compensation to the person so affected.

**59. Provision of false information by the subscriber:** (1) Any subscriber who:
(a) provides information to a certification service provider knowing such information to be false or not believing it to be correct to the best of his knowledge and belief;
(b) fails to bring promptly to the knowledge of the certification service provider any change in circumstances as a consequence whereof any information contained in a certificate accepted by the subscriber or authorized by him for publication or reliance by any person, ceases to be accurate or becomes misleading;
(c) knowingly causes or allows a certificate or his electronic signatures to be used in any fraudulent or unlawful manner, shall be guilty of an offence under this Act.
(2) The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding five years, or with fine which may extend to five hundred thousand rupees, or both.

60. Issue of false certificate: (1) Every director, secretary and other responsible officer, by whatever designation called, connected with the management of the affairs of a certification service provider, which:
(a) issues, publishes or acknowledges a certificate containing false or misleading information;
(b) fails to revoke or suspend a certificate after acquiring knowledge that any information contained therein has become false or misleading;
(c) fails to revoke or suspend a certificate in circumstances where it ought reasonably to have been known that any information contained in the certificate is false or misleading;

(d) issues a certificate as accredited certification service provider while its accreditation is suspended or revoked; shall be guilty of any offence under this Act.
(2) The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding five years, or with fine which may

extend to one million rupees, or with both.
(3) The certification service provider or its employees specified in sub-section (1), shall also be liable, upon conviction, to pay compensation for any foreseeable damage suffered by any person or subscriber as a direct consequence of any of the events specified in clauses (a) to (d) of sub-section (1).

61. Punishment **for commission of other offences:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in commission of any offence under any law in force in Pakistan, shall be punishable in accordance with the violated offence.

**62. Abetting, aiding or attempting any offence:** (1) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in abetting, aiding or attempting in the commission of offences provided under this Act or otherwise in any other law applicable and in force in Pakistan, shall be punishable in accordance with the violated offence.

**63.** Liability **to pay compensation:** (1) Any person who commits offences provided for under this Act shall further be liable to pay compensation to the person so affected.
(2) The compensation mentioned in sub-section (1) shall be recoverable as arrears of land revenue.

64. **Offences to be non-bailable, compoundable and** cognizable: (1) All offences under this Act shall be non-bailable, compoundable and cognizable.

CHAPTER VII- MISCELLANEOUS

**65. Application to acts done outside Pakistan:** (1) The provisions of this Act shall apply notwithstanding the matters being the subject hereof occurring outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons, information systems or events within the territorial jurisdiction of Pakistan.
66. Overriding effect: (1) The provisions of this Act shall apply notwithstanding anything to the contrary contained in any other law for the time being in force.

**67. Limitation on liability of network** service providers: (1) In the absence of intent to facilitate, aid or abet, a network service provider shall not be subject to any civil or criminal liability solely for the reason of use of his telecommunication system in connection with a contravention of this Act by a person not subject to the direction or control of the network service provider.
Explanation.—Telecommunication system in this section shall have the meaning given thereto under the Pakistan Telecommunication (Re-organisation) Act,

**1996 (XVII of 1996).**
**68. Limitation of liability of intermediaries:** (1) Notwithstanding anything contained in any law for the time being in force but subject **to** the provisions of sub sections (2) and **(3),** an intermediary shall not be liable for any third party information, data or communication link made available or hosted by him.
(2) The provisions of sub-section (1) shall apply *if:*
(a) the function of the intermediary is limited to providing access to an electronic device over which information made available by third parties is transmitted or temporarily store or host; or
(b) the intermediary does not initiate the transmission, selects the receiver of the transmission, and selects or modifies the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
(3) The provisions of sub-section (1) shall not apply if:
(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorize in the commission in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the Federal Government or its agency that any information, data or communication link residing in or connected to an electronic device, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

**69. Immunity against disclosure of information relating to** security **procedure: (1)** Subject to sub-section (2), no person

shall be compelled to disclose any password, key or other secret information exclusively within his private knowledge, which enables his use of the security procedure or advanced electronic signature.
(2) Sub-section (1) shall not confer any immunity where such information is used for the commission of any offence under any law for the time being in force.

70. Power to make regulations: (1) The Federal Government may, by notification in the official Gazette, make rules to carry out the Purposes of this Act and other ancillary matters thereto including, but not limited to, all matters in relation to the Cyber Authority, the Cyber Emergency Response Team and the Cyber Tribunal.

**71. Power to amend schedule:** (1) The Federal Government or the Cyber Authority may amend or make the schedules attached with Act in order to carry out the Purposes of this Act and other matters corrected thereto.

72. Prior publication of regulations: (1) All rules and regulations proposed to be made by the Federal Government and the cyber authority under this Act shall be published in the official Gazette and in at least one English and one Urdu daily with nationwide circulation, in draft form at least thirty days before the intended date of coming into operation.
(2) The Cyber authority shall keep record of all comments received on the draft of the rules or regulations, and shall prepare a report thereon addressing each comment.
(3) Th notification of the rules or regulations in their final form in the official Gazette shall be accompanied with a report of the cyber authority referred to in sub - section (2).

73. Removal of difficulties: (1) The Federal Government may by notification in the official Gazette, make provisions for removal of difficulties in a manner not inconsistent with the provisions of this Act.

CHAPTER VIII- REPEAL AND SAVINGS

74. Application of Act No. XVII **of** 1996: (1) Notwithstanding anything contained in the Pakistan Telecommunication (Re-organisation) Act, 1996 (XVII of 1996), the Cyber Authority shall be exclusively responsible for the functions described this Act and rules made hereunder.
Provided that, the foregoing provision shall not affect the applicability or operation of the provisions of the Pakistan Telecommunication (Reorganisation) Act, 1996 (XVII of 1996) to the telecommunication systems or telecommunication services, other than cryptography services, provided by the cryptography service providers.

75. Amendment of Act XVII **of** 1996: (1) In the Pakistan Telecommunication (Re-organisation) Act, 1996 (XVII of 1996), clause (b) of sub-section (2) of section 57 shall be omitted.
(2) Any provision in any license issued by the Pakistan Telecommunication Authority under the aforesaid Act prohibiting the provision or use of cryptography services shall cease to have effect subject to provisions of this Act.

**76. Repeal of** Act **LI of 2002:** (1) The Electronic Transactions Ordinance
2002 (LI of 2002) shall stand repealed by virtue of this Act, hereinafter referred
to as the repealed Ordinance, except the following is saved:
(a) The Schedule made under Section 29 of the repealed Ordinance titled as Amendments in Qanun-e-Shahadat Order, 1984 (P.O. No. 10 of 1984).

**77. Application to certain laws barred:** (1) Subject to sub-section (2), nothing in this Act shall apply to:
(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (XXVI of 1881);
(b) a power-of-attorney under the Powers of Attorney Act, 1881 (VII of 1882);
(c) a trust as defined in the Trust Act 1882 (II of 1882), but excluding constructive, implied and resulting trusts;
(d) a will or any form of testamentary disposition under any law for the time being in force; and
(e) a contract for sale or conveyance of immovable property or any interest in such property.
(2) The Federal Government after consultation with the Provinces may, by notification in the official Gazette and subject to such conditions and limitations as may be specified therein, declare that the whole or part of this Act shall apply to the whole or part of one or more instruments specified in clauses (a) to (e) of sub-Section (1).

**SCHEDULE - I**

(1) The Cyber Authority shall, with the prior approval of the Federal Government, prescribe regulations to carry out the purpose of this Act.
(2) Without prejudice to the generality of the sub-section (1), regulations may provide for:
(a) safety, control or management of keys, passwords or other secret information relating to certification service providers;
(b) standards, procedures and practices for time and date stamping;
(c) minimum qualifications of staff of certification service providers;
(d) adequacy of facilities and equipment for secure and reliable operation;
(e) privacy and protection of data of subscribers;
(f) inspection of operations;
(g) cross-certifications, accreditation, recognition, bridge certification or other arrangements with certification service

providers based in other countries;
(h) development of certification management system;
(I) reparation to subscribers for damage arising from negligence of certification service provider with conditions for and limits to liability;
(j) identification of areas of commerce or governance for use of certificates;
(k) standardization and technology relating to protocols, algorithms, interoperability of systems, applications and infrastructure for certification service providers;
(1) form and contents of applications for certification;
(m) suspension or revocation of certification;
(n) suspension or revocation of certification;
(o) certificate profiles with mandatory, optional and extension fields, if any;
(p) certificate revocation and suspension list profiles with mandatory and optional fields, and extension fields, if any;
(q) retention of records by certification authorities and the repository;

(r) recommended code of practice for handling and storage of business information and records in elections form; and
(s) regulation of access and audit trails.

**SCHEDULE -II**

(1) The Cyber Authority shall prescribe regulations for in respect of the certification practice statement as provided for under this Act.
(2) Without prejudice to the generality of the sub-section (1), regulations may provide for:
(a) prompt information to persons likely to be adversely affected by any event relating to the information system of the certification service provider or inaccuracy, invalidity or misrepresentation contained in a certificate;
(b) identification of subscribers;
(c) suspension or revocation of certificates;
(d) accuracy of information contained in a valid accreditation certificate;
(e) foreseeability of reliance on valid accreditation certificates;
(f) deposit of certificates or notification of any suspension or revocation of any accreditation certificate or any other fact or circumstance affecting the certificate, in the repository;
(g) form and procedure for submission of the certificate practice statement;
(h) mode of subsequently altering the approved certification practice statement;
(i) maintenance of the certification practice statement;
(j) inspection of the certification practice statement by the public;