3. Unauthorized access to information system or data.— Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

4. Unauthorized copying or transmission of data.— Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both.

5. Interference with information system or data.— Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

6. Unauthorized access to critical infrastructure information system or data.— Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

7. Unauthorized copying or transmission of critical infrastructure data.— Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both.

8. Interference with critical infrastructure information system or data.— Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both.

9. Glorification of an offence.— (1) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both. Explanation.—For the purposes of this section "glorification" includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism.— Whoever commits or threatens to commit any of the offences under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,— (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance interfaith, sectarian or ethnic hatred; or Page 7 of 25 (c) advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

11. Hate speech.—Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance interfaith, sectarian or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

12. Recruitment, funding and planning of terrorism.—Whoever prepares or disseminates information, through any information system or device, that invites or motivates to fund, or recruits people for terrorism or plans for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

13. Electronic forgery.— (1) Whoever interferes with or uses any information system, device or data, with the intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to two hundred and fifty thousand rupees or with both. (2) Whoever commits offence under subsection (1) in relation to a critical infrastructure information system or data shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to five million rupees or with both.

14. Electronic fraud.—Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.

15. Making, obtaining, or supplying device for use in offence. — Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shall, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months or with fine which may extend to fifty thousand rupees or with both.

16. Unauthorized use of identity information.— (1) Whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both. (2) Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information referred to in subsection (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information. Page 8 of 25

17. Unauthorized issuance of SIM cards etc.—Whoever sells or otherwise provides subscriber identity module (SIM) card, reusable identification module (RIUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

18. Tampering, etc. of communication equipment.—Whoever unlawfully or without authorization changes, alters, tampers with or reprograms unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both. Explanation.—A "unique device identifier" is an electronic equipment identifier which is unique to a communication device.

19. Unauthorized interception.— Whoever with dishonest intention commits unauthorized interception by technical means of— (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an

information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

20. Offences against dignity of a natural person.— (1) Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that nothing under this subsection shall apply to anything aired by a broadcast media or distribution service licensed under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002). (2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

21. Offences against modesty of a natural person and minor.—(1) Whoever intentionally and publicly exhibits or displays or transmits any information which,— Page 9 of 25 (a) superimposes a photograph of the face of a natural person over any sexually explicit image or video; or (b) includes a photograph or a video of a natural person in sexually explicit conduct; or (c) intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or (d) cultivates, entices or induces a natural person to engage in a sexually explicit act, through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both. (2) Whoever commits an offence under subsection (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees: Provided that in case of a person who has been previously convicted of an offence under sub‐section (1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine. (3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

22. Child pornography.—(1) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts— (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct; or (d) discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both. (2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data. Page 10 of 25

23. Malicious code.—Whoever willfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both. Explanation.—For the purpose of this section, the expression "malicious code" includes, a computer program or a hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.

24. Cyber stalking.— (1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information system network, the Internet, website, electronic mail or any other similar means of communication to— (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; (b) monitor the use by a person of the internet, electronic mail, text message or any other form of electronic communication; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person. (2) Whoever commits the offence specified in subsection (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that if victim of the cyber stalking under subsection (1) is a minor the punishment may extend to five years or with fine which may extend to ten million rupees or with both. (3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

25. Spamming.— (1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing. Page 11 of 25 (3) Whoever commits the offence of spamming as described in subsection (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be punished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend upto rupees five million or with both. (4) Whoever commits the offence of spamming as described in subsection (1) by transmitting unsolicited information, or engages in direct marketing in violation of subsection (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend up to one million rupees.

26. Spoofing.— (1) Whoever with dishonest intention establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing. (2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

1. GENERAL MORAL IMPERATIVES.

1.1 Contribute to society and human well-being.
1.2 Avoid harm to others.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Honor property rights including copyrights and patent.
1.6 Give proper credit for intellectual property.
1.7 Respect the privacy of others.
1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
2.2 Acquire and maintain professional competence.
2.3 Know and respect existing laws pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Honor contracts, agreements, and assigned responsibilities.
2.7 Improve public understanding of computing and its consequences.
2.8 Access computing and communication resources only when authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE.

4.1 Uphold and promote the principles of this Code.
4.2 Treat violations of this code as inconsistent with membership in the ACM.

Figure 19.6 ACM Code of Ethics and Professional Conduct

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.7 IEEE Code of Ethics

In recognition of my obligation to management I shall:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Figure 19.8 AITP Standard of Conduct