ETHICS IN INFORMATION TECHNOLOGY

Computer ethics refers to standards of moral conduct demonstrated in information technology related matters. It may address the following practices:

(i) Scavenging Techniques: Some browses through garbage for information that can be used to perform a criminal activity. In one case a scavenger looked through trash-cans containing computer output and illegally ordered thousands of dollars worth of communications equipment before being caught.

(ii) Leakage: Leakage results when important data, programs or computer resources normally safe-guarded leave a site without reason.

(iii) Eaves Dropping : Eaves dropping allows a person to observe transmissions intended for other people. Micro to main frame telecommunication links and local area networks are unreliable to eaves droppers. The primary targets of eaves dropper are protected passwords and account numbers.

(iv) Wire tapping : Wire tapping is a special case of eaves dropping, consists of setting up a special transmission path to direct the flow of data. In this case, an wire/cable can be illegally attached to a network to

perform various unauthorized acts such as espionage, stealing programs, altering data and so on. Satellite facilities are especially vulnerable to wire tapping. Fibre optic cable may also be affected out of this activity.

(v) Software Piracy: Software piracy refers to unauthorized copying or use of programmes. The most familiar form software piracy is when people make unauthorized copies of such programmes as windows, SPSS etc. for their own use. The most costly form of software piracy to organizations, however is where professional thieves make thousands of copies of a software programme and sell them illegally.

(vi) Hacking: The term 'hacker' originally referred to computer professionals who solved complex computer problems. Today the term 'hacker' (or crackers – the term used in IT circles) has a negative meaning. Hacking is a computer crime in which the criminal breaks into a computer system.

(vii) Jamming: In this case, software routines are used to tie up the computer hosting of a web site so that legitimate visitors can not access the site.

(viii) Sniffing: It is form of eaves dropping which involves placing a piece of software to intercept information passing from an user to the computer hosting of an website which includes credit card number and other confidential data.

(ix) Spoofing: In this case fraudulent misrepresentations as other organizations by setting up false websites take place where frauds can collect confidential information from unsuspecting visitors to site.

Preventive measures:

The following preventive measures may be taken to combat the above mentioned unethical activities in relation to information technology.

(i) **Careful hiring of people:** The most logical way to prevent such activities is by hiring trustworthy people. Although this is not easy to spot future criminals but by way of reference check or background check, chances of wrong recruitment can be minimized.

(ii) **Separation of employee functions:** Crimes are difficult to commit when the entire function is broken into smaller components with separate responsibilities to separate persons. Job rotation may be helpful in this regard.

(iii) Restriction of system use

(iv) Protecting resources with passwords or other user authorization checks

(v) Encryption of data and programmes which is the process of disguising data or programmes in coded form so they can not be recognized

(vi) Monitoring system transaction

(vii) Conducting frequent audits