Unit-2 **Micro and Macro Ethics**

In this Unit, one will learn about:

Ethics for IT Professionals

Ethics for IT Users

The topics of understanding will be Legal and ethical use of information resource, Right to privacy act, electronic surveillance, Software Piracy, Information Piracy, in-appropriate use of computer resources and information.

Computer Ethics

Computers with Internet raise a host of difficult moral issues, many of them connected with basic moral concerns such as free speech, privacy, respect for property, informed consent and harm.

To evaluate and deal with these issues, a new area of applied ethics called Computer Ethics has come up.

These ethics are related to all the computer professionals such as programmers, analysts, operators, designers, etc. along with the users.

The ten commandments of Computer Ethics, created in 1992 by the Computer Ethics Institute consist of the following −

- One should never use a computer −
- To harm the people (anti-social activities)
- To interfere with other's work (illegal manipulations)
- To snoop into other's files (malware)
- To steal a computer/data (hacking)
- To bear false witness (manipulation and morphing)
- To use/ copy a software you didn't pay for (like illegal downloads and usages)
- To use or copy other's software without compensations (illegal pirated versions)
- To use other's intellectual output inappropriately (violating IPR)
- Doing without thinking of social consequences of the program being written (libeling)

Always use a computer ensuring consideration and respect towards fellow beings.

However, these ethics are facing lax in today's world. A very small section of concerned individuals seems to be following these ethics. A large section seems to be violating these ethics. With this, there is an unprecedented increase in cybercrime.

The most commonly discussed cases of computer abuse are instances such as −

- ✓ The stealing or cheating by employees at work.
- ✓ The stealing by non-employees or former employees.
- ✓ The stealing from or cheating clients and consumers.
- ✓ The violation of contracts for computers sales or services.
- ✓ The many conspiracies to use computer networks to engage in widespread fraud.

Ethics and the IT Professional

Just because you can do something doesn't mean you should do it. Like any other profession, information technology benefits from a standard, accepted code of ethics that helps guide behavior in sometimes confusing contexts.

IT Professional???

An IT Professional is a person having specialized knowledge who have undergone a intensive preparation on IT Skills and techniques.

Who can be an IT Professional?

Many workers in the IT industry are considered to be professionals. A partial list includes:

- Programmers/Analysts
- Software engineers
- Database administrators
- Network administrators
- Computer Operators
- Computer Salesperson
- Computer Scientist
- Computer Technician
- Technical Writer
- Graphic Designer/Illustrator
- Web Developer
- Consultant
- Computer Trainer /Educator
- Computer Security Specialist
- Computer Forensic Specialist

Professional Relationships

IT professionals become involved in many different types of relationships.

Professional-employer
Professional-client
Professional-supplier
Professional-Professional (Peer-to-Peer)
Professional-IT user
Professional-society

Some of the ethical issues

Is it okay to read campus users' email?
What if you believe that university policies are being violated?
Would you tell the users that their email is being read?
Is it okay to look through files on a user's laptop when you're troubleshooting a problem?
What if the user is someone you think might be storing illegal content on the laptop?

If any of these questions caused you to stop and think about what you would do, you're not alone.

Ethical choices often seem murky. We live in a human society, subject to less-than-complete information, societal pressures, and multiple interpretations of facts.

More often than not, we need to apply professional judgment, which is guided by our own experiences as well as reliance on laws, policies, and culture.

Professional ethics is becoming more important in the workplace. As professionals become more specialised in their professional occupation, professional bodies have increasingly been busy developing, revising and refining professional codes of ethics.

Code of Behaviour

A Code of Behaviour is a set of conventional principles and expectations that are considered binding on a person who is a member of a particular group (such as a professional body). An ethical code generally implies documents at three levels:

- Code of business ethics;
- Codes of Conduct for employees; and
- Codes of professional practice.

Sources of Ethical Guidance for IT Professionals provided by various committees/organizations

- Association for Computing Machinery has its own code of ethics
- PMI (Project Management Institute) has its own conduct and code of ethics
- IEEE has code of ethics for publishing information and accessing information.
- Association of Information Technology Professionals (AITP) has code of ethics and standards of conduct.
- SANS has published IT code and ethics

In general these codes assert that IT professionals need to commit to:

- Integrity
- Competence
- Professional responsibilities
- Work responsibilities
- Societal responsibilities

Specific guidance stems from these general principles. Some common commitments between the three codes are to:

- Maintain technical competence
- Avoid injury to others, their property, reputation, or employment
- Reject bribes, kickbacks, etc.

Ethical behavior of IT Professionals

Professional Code of Ethics

States the principles and core values that are essential to the work of a particular occupational group.

Code of conduct has two main parts:

Aspirations of the organization

Rules and/or principles

Benefits:

Improves ethical decision making

Promotes high standard of practice and ethical behavior.

Provides a evaluation benchmark

IT Professional Malpractice

Negligence has been defined as not doing something that a reasonable man would do, or doing some that a reasonable man would not do.

Duty of care refers to the obligation to protect people against unreasonable harm or risk.

IT Users

Common ethical issues of IT users

- ✓ Software Piracy
- ✓ Information Piracy
- ✓ Inappropriate use of computing resources
- ✓ Inappropriate sharing of information

Supporting Ethical Practices of IT Users

- Define and limit the appropriate use of IT resources.
- Establish guidelines for the use of company software.
- Structure information systems to protect data and information.
- Install and maintain a corporate firewall.

Legal and ethical use of information

Ethical use of information means using information ethically.

Actually there are two ways that very clearly deal with this concept. They are plagiarism and copyright.

Both deal with giving credit where credit is due and using other people's work correctly. Even though information, words, and ideas are not concrete, they still can be stolen and those that do that can still get in trouble.

Cyber-crime

- Cyber-crime refers to the use of information technology to commit crimes. Cyber-crimes can range from simply annoying computer users to huge financial losses and even the loss of human life.

Information Communication Technology (ICT) policy

An ICT policy is a set of guidelines that defines how an organization should use information technology and information systems responsibly. ICT policies usually include guidelines on:

- ❖ Purchase and usage of hardware equipment and how to safely dispose them
- ❖ Use of licensed software only and ensuring that all software is up to date with latest patches for security reasons

- Rules on how to create passwords (complexity enforcement), changing passwords, etc.
- Acceptable use of information technology and information systems
- Training of all users involved in using ICT and MIS

Software Piracy
What is Software Piracy?

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen.

Types of Software Piracy

Softlifting
The most common type of piracy, softlifting, (also called softloading), means sharing a program with someone who is not authorized by the license agreement to use it.

A common form of softlifting involves purchasing a single licensed copy of software and then loading the software onto several computers, in violation of licensing terms.

On college campuses, it is rare to find a software program that has not been softloaded.

People regularly lend programs to their roommates and friends, either not realizing it's wrong, or not thinking that it's a big deal.

Softlifting is common in both businesses and homes.

Hard disk loading

Often committed by hardware dealers, this form of piracy involves loading an unauthorized copy of software onto a computer being sold to the end user.

This makes the deal more attractive to the buyer, at virtually no cost to the dealer. The dealer usually does not provide the buyer with manuals or the original CDs of the software.

This is how operating systems, like Windows are often pirated.

Renting

Renting involves someone renting out a copy of software for temporary use, without the permission of the copyright holder.

The practice, similar to that of renting a video from Blockbuster, violates the license agreement of software.

OEM unbundling

Often just called "unbundling," this form of piracy means selling stand-alone software originally meant to be included with a specific accompanying product. An example of this form of

piracy is someone providing drivers to a specific printer without authorization.

Counterfeiting

Counterfeiting means producing fake copies of a software, making it look authentic. This involves providing the box, CDs, and manuals, all designed to look as much like the original product as possible.

Microsoft products are the ones most commonly counterfeited, because of their widespread use. Most commonly, a copy of a CD is made with a CD-burner, and a photocopy of the manual is made.

Counterfeit software is sold on street corners, and sometimes unknowingly sold even in retail stores. Counterfeit software is sold at prices far below the actual retail price.

Consequences of Software Piracy

The losses suffered as a result of software piracy directly affect the profitability of the software industry.

Consequently, software publishers, developers, and vendors are taking serious actions to protect their revenues.

Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated

software forfeit some practical benefits as well. Those who use pirate software:

- Increase the chances that the software will not function correctly or will fail completely;
- Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
- Have no warranty to protect themselves;
- Increase their risk of exposure to a debilitating virus that can destroy valuable data;
- May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
- Are subject to significant fines for copyright infringement; and
- Risk potential negative publicity and public and private embarrassment.

To Stay Safe Online

- Avoiding phishing scams:
- Don’t reply to emails, text messages, or pop-ups that ask for personal information.

- Don't respond if you get a message - by email, text, pop-up or phone - that asks you to call a phone number to update your account or give your personal information to access a refund.

- Only disclose personal information to trusted or secure websites.

- Change your passwords regularly.

Implications of sharing of inappropriate information

Facebook data scandal: Social network fined $5bn over 'inappropriate' sharing of users' personal information

The FTC has been investigating allegations Facebook inappropriately shared information belonging to 87 million users with the now-defunct British political consulting firm Cambridge Analytica.

The probe has focused on whether the sharing of data and other disputes violated a 2011 consent agreement between Facebook and the regulator.