1. What is Profession?

The subsequent discussion on the terms “job”, “occupation” and “profession” will help define the term “profession”. Let’s have eyes on its attributes first: -

1.1. Attributes of Profession

There have been many studies on the nature of professions has been achieved. Attributes of a profession include: -

1. Work that requires sophisticated skills, the use of judgment, and the exercise of discretion. Also, the work is not routine and is not capable of being mechanized;
2. Membership in the profession requires extensive formal education, not simply practical training or apprenticeship;
3. The public allows special societies or organizations that are controlled by members of the profession to set standards for admission to the profession, to set standards of conduct for members, and to enforce these standards; and
4. Significant public good results from the practice of the profession.

In a profession, “judgment” refers to making significant decisions based on formal training and experience. In general, the decisions will have serious impacts on people’s lives and will often have important implications regarding the spending of large amounts of money.

“Discretion” can have two different meanings. The first definition involves being discrete in the performance of one’s duties by keeping information about customers, clients, and patients confidential. This confidentiality is essential for engendering a trusting relationship and is a hallmark of professions. The other definition of discretion involves the ability to make decisions autonomously. Many people are allowed to use their discretion in making choices while performing their jobs. However, the significance of the decision marks the difference between a job and a profession.

1.2. Examination of Different Occupations

Let’s examine athletes and carpenters in light of the foregoing definition of professions. An athlete who is paid for her appearances is considered to have sophisticated skills that most people do not possess, and these skills are not capable of mechanization. However, substantial judgment and discretion are not called for on the part of athletes in their “professional” lives, so athletics fails the first part of the definition of professional. Interestingly, though, professional athletes are frequently viewed as role models and are often disciplined for a lack of discretion in their personal lives.

Athletics requires extensive training, not of a formal nature, but more of a practical nature acquired through practice and coaching. No special societies are required by athletes, and athletics does not meet an important public need; although entertainment is a public need, it certainly doesn’t rank highly compared to the needs met by professions such as medicine. So, although they are highly trained and very well compensated, athletes are not professionals.

Similarly, carpenters require special skills to perform their jobs, but many aspects of their work can be mechanized and little judgment or discretions required. Training in carpentry is not formal, but rather is practical by way of apprenticeships. No organizations or societies are required. However carpenter certainly does meet an aspect of the public good—providing shelter is fundamental to society—although perhaps not to the same extent as do professions such as medicine. So, carpentry also doesn’t meet the basic requirements to be a profession.

Let's look at two occupations that are definitely regarded by society as professions: medicine and law. Medicine certainly fits the definition of a profession given previously. It requires very sophisticated skills that cannot be mechanized, it requires judgment as to appropriate treatment plans for individual patients, and it requires discretion. (Physicians have even been granted physician-patient privilege, the duty not to divulge information given in confidence by the patient to the physician). Although medicine requires extensive practical training learned through an apprenticeship called a residency, it also requires much formal training (four years of undergraduate school, three to four years of medical school, and extensive hands-on practice in patient care), Medicine has a special society (e.g. Nepal Medical Council) to which a large fraction of practicing physicians belong and that participates in the regulation of medical schools, sets standards for practice of the profession, and enforces codes of ethical behaviour for its members. Finally, healing the sick and helping to prevent disease clearly involve the public good. By the definition presented previously, medicine clearly qualifies as a profession.

Similarly, law is a profession. It involves sophisticated skills acquired through extensive formal training; has a professional society, the Nepal Bar Association; and serves an important aspect of the public good.

The difference between athletics and carpentry on one hand and law and medicine on the other is clear. The first two really cannot be considered professions, and the latter two most certainly are.

2. Is Engineering a Profession?

People use terms different terms like "Job", "Occupation" or "Profession" to refer to a work. Any work for hire can be considered a job, regardless of the skill level involved and the responsibility granted. Engineering is certainly a job - engineers are paid for their services - but the skills and responsibilities involved in engineering make it more than just a job.

Similarly, the word "occupation" implies employment through which someone makes a living. Engineering, then, is also an occupation. There are no amateur engineers who perform engineering work without being paid while they train to become professional, paid engineers. Likewise, the length of time one works at an engineering related job, such as air engineering aide or engineering technician, does not confer professional status no matter how skilled a technician one might become.

Engineering is a profession because: -

- ? It needs extensive and formal education / training
- ? Engineering design requires sophisticated skills that can not be mechanized. (Only the construction after the design could be mechanized.)
- ? Engineering design involves a remarkable amount of judgement and discretion.
- ? Engineers have societies (e.g. IEEE, ACM etc.) which set standards for engineering practice and code of ethics for the professionals.
- ? They produce publicly important results like bridges, automated machines etc.

3. Professional Responsibilities

We will begin our discussion of professional rights and responsibilities by first looking more closely at a few of the important responsibilities that engineers have.

3.1. Confidentiality and Proprietary Information

A hallmark of the professions is the requirement that the professional keep certain information of the client secret or confidential. Confidentiality is mentioned in most engineering codes of ethics. This is a well-established principle in professions such as medicine, where the patient's medical information

must he kept confidential, and in law, where attorney-client privilege is a well-established doctrine. This requirement applies equally to engineers, who have an obligation to keep proprietary information of their employer or client confidential.

Most information about how a business is run, its products and its suppliers, directly affects the company's ability to compete in the marketplace. Such information can be used by a competitor to gain advantage or to catch up. Thus, it is in the company's (and the employee's) best interest to keep such information confidential to the extent possible.

Some information obviously needs to be kept confidential viz. test results and data, information about upcoming unreleased products, and designs or formulas for products. Engineers working for a client are frequently required to sign a nondisclosure agreement. Of course, those engineers working for the government, especially in the defence industries have even more stringent requirements about secrecy placed on them and may even require a security clearance granted after investigation by a governmental security agency before being able to work.

However, there are grey areas that must he considered. For example, a common problem is the question of how long confidentiality extends after an engineer leaves employment with a company. Legally, an engineer is required to keep information confidential even after she has moved to a new employer in the same technical area. In practice, doing so can be difficult. Even if no specific information is divulged to a new employer, an engineer takes with her a great deal of knowledge of what works, what materials to choose, and what components not to choose. This information might be considered proprietary by her former employer. However, when going to a new job, an engineer cannot be expected to forget all of the knowledge already gained during years of professional experience.

The courts have considered this issue and have attempted to strike a balance between the competing needs and rights of the individual and the company. Individuals have the right to seek career advancement wherever they choose, even from a competitor of their current employer. Companies have the right to keep information away from their competitors. The burden of ensuring that both of these competing interests are recognized and maintained lies with the individual engineer.

3.2. Conflict of Interest

Avoiding conflict of interest is important in any profession, and engineering is no exception. A conflict of interest arises when an interest, if pursued, could keep a professional from meeting one of his obligations. For example, a civil engineer working for a state department of highways might have a financial interest in a company that has a bid on a construction project. If that engineer has some responsibility in determining which company's bid to accept, then there is a clear conflict of interest. Pursuing his financial interest in the company might lead him not to objectively and faithfully discharge his professional duties to his employer, the highway department. This type of conflict of interest is called **actual conflicts of interest**.

There are two more types of conflicts of interest. The second type is **potential conflicts of interest**, which threaten to easily become actual conflicts of interest. For example, an engineer might find herself becoming friends with a supplier for her company. Although this situation doesn't necessarily constitute a conflict, there is the potential that the engineer's judgement might become conflicted by the needs to maintain the friendship.

Finally, there are situations in which there is the **appearance of a conflict of interest**. This might occur when an engineer is paid based on a percentage of the cost of the design. There is clearly no incentive to cut costs in this situation, and it may appear that the engineer is making the design more expensive simply to generate a larger fee. Even eases where there is only an appearance of a conflict of interest can be significant, because the distrust that comes from this situation compromises the engineers ability to do this work and future work and calls into question the engineer's judgement.

A good way to avoid conflicts of interest is to follow the guidelines of company policy. In the absence of such a policy; asking a co-worker or your manager will give you a second opinion and will make it clear that you aren't trying to hide something. In the absence of either of these options, it is best to examine your motives and use ethical problem-solving techniques. Finally, you can look to the statements in the professional ethics codes that uniformly forbid conflicts of interest.

3.3. Environmental Ethics

The environmental movement has sought to control the introduction of toxic and unnatural substances into the environment, to protect the integrity of the biosphere, and to ensure a healthy environment for humans. Engineers are responsible in part for the creation of the technology that has led to damage of the environment and are also working to find solutions to the problems caused by modem technology. The environmental movement has led to an increased awareness among engineers that they have a responsibility to use their knowledge and skills to help protect the environment. This duty is even spelled out in the code of ethics of the IEEE.

Fundamental to discussing ethical issues in environmentalism is a determination of the moral standing of the environment. The Western ethical tradition is anthropocentric, meaning that only human beings have moral standing. Animals and plants are important only in respect to their usefulness to humans. If animals, trees, and other components of the environment have no moral standing, then we have no ethical obligations towards them beyond maintaining their usefulness to humans. There are significant numbers of people who feel that the environment, and specifically animals and plants, do have standing beyond their usefulness to humans. In one form, this view holds that humans are just one component of the environment and that all components have equal standing. For those who hold this view, it is an utmost duty of everyone to do what is required to maintain a healthy biosphere for its own sake.

4. Professional Rights

Engineers also have rights that go along with their responsibilities. Not all of these rights come about due to the professional status of engineering. They are rights that individuals have regardless of professional status, including the right to privacy, the right to participate in activities of one's own choosing outside of work, the right to reasonably object to company policies without fear of retribution, and the right to due process.

The most fundamental right of an engineer is the right of **professional conscience**. This involves the right to exercise professional judgement in discharging one's duties and to exercise this judgement in an ethical manner. This right is basic to an engineer's professional practice.

The right of professional conscience can have many aspects. For example, one of these aspects might he referred to as the **Right of Conscientious Refusal.** This is the right to refuse to engage in unethical behaviour. Put quite simply, no employer can ask or pressure an employee into doing something that she considers unethical and unacceptable. For example, an engineer ought to be allowed to refuse to work on defence projects or environmentally hazardous work if his conscience says that such work is immoral.

5. Codes of Ethics and Professional Conduct

Codes of ethics serve a variety of functions. A code of ethics may, at one and the same time, be directed to members of the profession, the public and employers and clients of members of the profession.

Perhaps the most important function of a code of ethics is as a statement embodying the collective wisdom of members of the profession. You can read a code of ethics as a statement of what members of the profession, with many years of experience, have found to be the most important things to think

about and do when working as a computer professional. The code expresses both the experience of many members and the consensus of many members.

Currently, there are several codes of ethics in computer. Perhaps the most visible codes are those produced by the ACM and the IEEE. The Software Engineering Codes of Ethics and Professional Practice were developed by a joint ACM-IEEE taskforce with an eye to the licensing of software engineers.

5.1. The Institute of Electrical and Electronics Engineers, Inc. (IEEE)

We, the members of the IEEE, in recognition of the importance of our technologies 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 engineering 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.

Approved by the IEEE Board of Directors, August 1990.

5.2. ACM Code of Ethics and Professional Conduct

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.
The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.
It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. GENERAL MORAL IMPERATIVES.

As an ACM member, I will....

1.1 Contribute to society and human well-being.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.
In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

1.2 Avoid harm to others.

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, co-workers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the

problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5: regarding thorough evaluations.

1.3 Be honest and trustworthy.
Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems. A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.
The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honour property rights including copyrights and patent.
Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behaviour. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

1.6 Give proper credit for intellectual property.
Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

1.7 Respect the privacy of others.
Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including

electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honour confidentiality.
The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honour confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

As an ACM computing professional I will ....

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence.
Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work.
ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.
Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm,including the reporting of professional violations.

2.6 Honour contracts, agreements, and assigned responsibilities.
Honouring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.
However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences.
Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.
Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

As an ACM member and an organizational leader, I will ....
3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

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.
Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.
This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. COMPLIANCE WITH THE CODE.

As an ACM member I will ....
4.1 Uphold and promote the principles of this Code.
The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM.
Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.
This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

6. Whistleblowing

Whistleblowing is the act by an employee of informing the public or higher management of unethical or illegal behaviour by an employer or supervisor. There are frequent newspaper reports of cases in which an employee of a company has gone to the media with allegations of wrongdoing by his or her employer or in which a government employee has disclosed waste or fraud.

According to the codes of ethics of the professional engineering societies, engineers have a duty to protect the health and safety of the public, so in many cases, an engineer is compelled to blow the whistle on acts or projects that harm these values, Engineers also have the professional right to disclose wrongdoing within their organizations and expect to see appropriate action taken.

6.1. Types of Whistleblowing

A distinction is often made between internal and external whistleblowing. **Internal Whistleblowing** occurs when an employee goes over the head of an immediate supervisor to report a problem to a higher level of management. Or, all levels of management are bypassed, and the employee goes directly to the president of the company or the board of directors, However it is done, the whistleblowing is kept within the company or organization. **External Whistleblowing** occurs when the employee goes outside the company and reports wrongdoing to newspapers or law-enforcement authorities. Either type of whistleblowing is likely to be perceived as disloyalty. However, keeping it within the company is often seen as less serious than going outside of the company.

There is also a distinction between acknowledged and anonymous whistleblowing. Anonymous whistleblowing occurs when the employee who is blowing the whistle refuses to divulge his name when making accusations. These accusations might take the form of anonymous memos to upper management or of anonymous phone calls to the police. The employee can also talk to the news media but refuse to let her name be used as the source of the allegations of wrongdoing. Acknowledged whistleblowing, on the other hand, occurs when the employee puts his name behind the accusations and is willing to withstand the scrutiny brought on by his accusations.

Whistleblowing can be very bad from a corporation point of view because it can lead to distrust, disharmony, and an inability of employees to work together. Similarly, in business, whistleblowing is perceived as an act of extreme disloyalty to the company and to co-workers.

6.2. When Should Whistleblowing Be Attempted?

Whistleblowing should only be attempted if the following four conditions are met:

6.2.1. Need.

There must be a clear and important harm that can be avoided by blowing the whistle. In deciding whether to go public, the employee needs to have a sense of proportion. You do not need to blow the whistle about everything, just the important things Of course, if there is a pattern of many small things that are going on, this can add tip to a major and important matter requiring that the whistle be blown.

6.2.2. Proximity

The whistleblower must be in a very clear position to report on the problem. Hearsay is not adequate. Firsthand knowledge is essential to making an effective case about wrongdoing. This point also implies that the whistleblower must have enough expertise in the area to make a realistic assessment of the situation. This condition stems from the clauses in several codes of ethics that mandate that an

engineer not undertake work in areas outside her expertise. This principle applies equally well to making assessments about whether wrongdoing is taking place.

6.2.3. Capability

The whistle blower must have a reasonable chance of success in stopping the harmful activity. You are not obligated to risk your career and the financial security of your family if you can't see the case through to completion or you don't feel that you have access to the proper channels to ensure that the situation is resolved.

6.2.4. Last Resort

Whistleblowing should be attempted only if there is no one else more capable or more proximate to blow the whistle and if you feel that all other lines of action within the context of the organization have been explored and shut off.

6.3. Preventing Whistleblowing

There are four ways in which to solve the whistleblowing problem within a corporation.

First, there must he a **strong corporate ethics culture**. This should include a clear commitment to ethical behaviour, starting at the highest levels of management, and mandatory ethics training for all employees. All managers must set the tone for the ethical behaviour of their employees.

Second, there should be **clear lines of communication** within the corporation. This openness gives an employee who feels that there is something that must be fixed a clear path to air his concerns.

Third, all employees must have **meaningful access to high-level managers** in order to bring their concerns forward. This access must come with a guarantee that there will be no retaliation. Rather, employees willing to come forward should be rewarded for their commitment to fostering the ethical behaviour of the company.

Finally, there should be willingness on the part of management to **admit mistakes**, publicly if necessary. This attitude will set the stage for ethical behaviour by all employees.

Source:

- Deborah G. Johnson, *Computer Ethics*, Third Edition
- Charles B. Fleddermann, *Engineering Ethics*, Second Edition