Question#01

ACM Code of Ethics

1. General Ethical Principles:

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefits of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy.

1.2 Avoid Harm

"Harm" means negative consequences, especially when those consequences are significant and unjust.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm.

1.3 Be honest and thtrustwovthy

Honesty is an essential component of thevustwovthiness. A computing pvofessional should be tvanspavent and pvovide full disclousevе of all pevtinent system capabilities, limitations, and potential pvoblems to the appvopviate visk.

Computing pvofessionals should be honest about their qualifiations, and about any limitations in their competence to complete a task.

1.4 Be fair and take action not to discviminate

The values of equality, tolevence, vespect fov othevs and justice govevn this pvinciple. Fairness vequires that even cavepul decisions pvocesses pvovide some avenue of vedvess of gvievances.

1.5. Respect the wovk vequived to produce new ideas, inventions, creative wovks, and computing avtifacts.

Developing new ideas, inventions, creative wovks, and computing avtifacts cveates value fov society, and those who expand their effovt should expect to gain value fvom their wovk.

Computing pvofessionals should thevefove credit their cveatovs of ideas, inventions, wovk, and avtifacts and vespects copyvights, patents, tvade secvets, license agveements and other methods of pvotecting authov's wovks.

1.6 Respect Privacy

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring and exchange of personal information quickly, inexpensively and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

1.7 Honor Confidentiality

Computing professionals are often entrusted with confidential information. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the code. In these cases, the nature of content should not be disclosed except to appropriate authorities.

2. Professional Responsibilities

2.1 Strive to achieve high quality in both the processes and products of professional work.

Computing professionals should insist on and support high quality work from themselves and from colleagues. The dignity of employers, employees, colleagues, clients, users and anyone else affected either directly or indirectly by the work should be respected throughout the work(process). Computing professionals should respect the right of those involved to transparent communication about the project.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis and in recognizing and navigating ethical challenges.

2.3 Know and respect existing rules pertaining to professional work.

"Rules" here include local, regional, national and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A computing professional who decides to violate a rule because it is unethical, or for any reason, must consider potential consequences and accept responsibility for that action.

2.4 Accept and provide appropriate professional review.

High quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations and testimony to employers, employees, clients, users and the public. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning system.

2.6 Perform work only in areas of competence

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility, and making a judgment about whether the work assignment is within the professional's area of competence. If at any time before or during the work assignment (~~is execution~~) the professional identifies a lack of necessary expertise, they must disclose this to the employer or client.

2.7. Foster public awareness and understanding of computing, related technologies, and their consequences.

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impact of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the code. Consequently, computing professionals should not access another's computer system, software or data without a reasonable belief that such an action would be authorized or compelling belief that it is consistent with the public good.

2.9 Design and implement systems that are robustly and usably secure.

To ensure the system achieves its intended purpose, security feature should be designed to be as intuitive and easy to use as possible. Computing professionals should discourage security precautions that are too confusing, are situationally inappropriate, or otherwise inhibit legitimate use.

In cases where misuse or harm are predictable or unavoidable, the best option may not implement the system.

3. Professional Leadership Principles

3.1 Ensure that the public good is the central concern during all professional computing work.

People - including users, customers, colleagues, and others affected directly or indirectly - should always be the central concern in computing. The public good should always an explicit consideration when evaulting tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they used in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizations reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to enhance the quality of working life.

Leader should ensure that they enhance, not degrade, the quality of working life. Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the code.

Leaders should pursue clearly defined organizational policies that are consistent with the code and effectively communicate them

to relevant stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated. Designing or implementing processes that deliberately or negligently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.

3.5. Create opportunities for members of the organization or group to grow as professionals.

Education opportunities are essential for all organization and members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in technical specialities. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular systems.

3.6 Use care when modifying or retiring systems.

Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work. Leaders should take care when changing or discontinuing support for system features on which people still depend. Leaders should thoroughly investigate viable alternatives to removing support for a legacy system.

If these systems's alternatives are unacceptably risky or impractical, the developer should assist stakeholders' graceful migration from the system to alternative.

3.7 Recognize and take special care of system that become integrated into the infrastructure of society.

Even the simplest computer system have the potential to impact all aspects of society when integrated with everyday activities which organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded.

4. Compliance with the Code

4.1 Uphold, promote, and respect the principles of the code.

The future of computing depends on both technical and ethical excellence. Computing Professionals should adhere to the principles

of the Code and contribute to improving them. Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, including, when reasonable, expressing their concern to the person or persons thought to be violating the Code.

4.2 Treat violations of the code as inconsistent with membership in the ACM.

Each ACM member should encourage and support adherence by all computing professionals regardless of ACM memberships. ACM members who recognize a breach of the Code should consider reporting the violation to the ACM, which may result in remedial action as specified in the ACM's Code of Ethics and Professional Conduct Enforcement Policy.