CS 100 Lab 02 – ACM Code of Ethics

https://www.acm.org/code-of-ethics

1. GENERAL ETHICAL PRINCIPLES

A computing professional should...

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
1.2 Avoid harm.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
1.6 Respect privacy.
1.7 Honor confidentiality.

2. PROFESSIONAL RESPONSIBILITIES

A computing professional should...

2.1 Strive to achieve high quality in both the processes and products of professional work
2.2 Maintain high standards of professional competence, conduct, and ethical practice.
2.3 Know and respect existing rules 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 Perform work only in areas of competence.
2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.
2.8 Access computing and communication resources only when authorized or when compelled by the public good.
2.9 Design and implement systems that are robustly and usably secure.

3. PROFESSIONAL LEADERSHIP PRINCIPLES

A computing professional should...

3.1 Ensure that the public good is the central concern during all professional computing work.
3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.
3.3 Manage personnel and resources to enhance the quality of working life.
3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.
3.5 Create opportunities for members of the organization or group to grow as professionals.
3.6 Use care when modifying or retiring systems.
3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

4. COMPLIANCE WITH THE CODE

A computing professional should...

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

For each case study, identify which principles of the Code are most relevant. Consider both positive support of the code and possible violations of the code. Submit your team names and answers in the online form.

Case Study A - Medical Implant Risk Analysis

ABC is a medical technology startup that builds an implantable heart health monitoring device. The device comes with a smart phone app that monitors and controls the device wirelessly, as well as stores a persistent record that can be shared with medical providers. After being approved by multiple countries' medical device regulation agencies, ABC quickly gained market share based on the ease of use of the app and the company's vocal commitment to securing patients' information. To further expand their impact, ABC worked with several charities to provide the device at a reduced price to patients living below the poverty line.

As a basic security mechanism, ABC's implant could only be accessible through short-range wireless connections, requiring the phone and implant to be in close proximity. Data transferred between the app and the device employed standard cryptographic algorithms, and all data stored on the phone was encrypted. To support on-going improvement, ABC had an open bug bounty program inviting disclosure of potential vulnerabilities in their app.

At a recent security conference, an independent researcher claimed to have found a vulnerability in the wireless connectivity. The researcher presented a proof-of-concept demonstration where a second device in close proximity could modify commands sent to the implant to force a device reset. The attack relied on the use of a hard-coded initialization value stored in the implant device that created a predictable pattern in the data exchanges that could be manipulated. In consultation with ABC's technical leaders, the researcher concluded that the risk of harm with this attack is negligible, given the limited capabilities of the device.

Case Study B - Abusive Workplace Behavior

Diane recently started a new industry research job, joining the company's interactive technologies team. In graduate school, her advisor had collaborated with several members of the team on a few research projects, involving and highlighting Diane's contributions whenever possible. The team had been impressed by Diane's work and recruited her as she was approaching graduation.

Max, the team's technical leader, had built a reputation as a brilliant yet mercurial expert in augmented reality. His team's contributions were highly cited within the field, with Max typically claiming primary authorship as the team leader. Their work was also highlighted frequently in the popular press, always with quotes only from Max. Despite the team's repeated successes, Max would erupt with verbal and personal attacks for even minor mistakes. He would yell at the person and berate them in internal chat forums. On multiple occasions, team members—only the women—have found their names removed from journal manuscript submissions as punishment.

Diane soon found herself the target of one of Max's tirades when she committed a code update that introduced a timing glitch in the prototype shortly before a live demo. Infuriated, Max refused to allow Diane to join the team onstage. Feeling Max's reaction was unprofessional and abusive, Diane approached the team's manager, Jean, who must consider how to respond.