

UNIVERSITY OF GUJRAT LAHORE SUB CAMPUS

Spring 2021

ANSWER BOOK

Student Name:	Rehman Ahmed
Student Roll Number:	17281519-050
Course Title:	Professional Practices
Course Code:	CS-341
Semester:	8
Degree Program:	BS CS

Start your paper here:

Q no 1

Tell your management that if the company is using pirated software for free, it would be only honest to freely distribute all the software produced by the company. Of course, it still wouldn't be ethical, the same way it is not ethical to give away the items you steal in a shop, but at least it would be equal.

Of course, your management will not do it but at least they might think about the issue. However, I doubt they'll do that, either - most probably, they will tell you to find another job if you don't like it there.

Anyway, it all starts with communication - find out what is the reasoning behind their behavior - why they are doing that and if there might be different solutions, for example, using open source tools, participating in start-up programs which give you access to lots of free software tools (Microsoft BizSpark) etc. But if they don't understand the problem and say: "Yeah, so what, everybody is doing this" then just leave that company. They are not worth having you working for them.

Q no 2

Real World Example:

If you doing a job in software company as an employee, then you should be clear about your moto. If you assigned by a task than before accepting it clearly checked and then told your manager that you can do it in that given period of time. Don't make so clever that you can do it in a single day. Take a proper time and then do it. Because if you did not complete it in a given deadline then that would be very bad impression from your side, also make sure that every task provided you is clearly understood and level of complexity should also keep in mind after that you can give proper time period of doing that task.

Q no 3

Ethical code asserts an ACM member will be “fair and take action not to discriminate”

This case highlights issues involving fairness and discrimination

In this case, system designer is asked to build a system that, it appears will be used to favour white males and discriminate against non-whites and females from this is would appear that:

System designer should not do what he or she is told, plus should also point out the problematic nature of what is being requested and ask client why this is being done

- If client answers that they plan to use information to favour white males, then:

Computer professional should refuse to build the system as proposed.

To go ahead and build the system would violate:

- 1 (fairness)
- 2 (respecting existing laws)
- It would also be inconsistent with:
 - 1 (well-being)
 - 2 (avoiding harm)

Q no 4

Empathic listening (also called active listening or reflective listening) is a way of listening and responding to another person that improves mutual understanding and trust. It is an essential skill for third parties and disputants alike, as it enables the listener to receive and accurately interpret the speaker's message, and then provide an appropriate response. The response is an integral part of the listening process and can be critical to the success of a negotiation or mediation. Among its benefits, empathic listening

1. builds trust and respect,
2. enables the disputants to release their emotions,
3. reduces tensions,
4. encourages the surfacing of information, and
5. creates a safe environment that is conducive to collaborative problem solving.

Q no 5

These professionals standards of personal must adhere to the highest and professional conduct to faithfully carry out their responsibilities, gain the respect of management and employees and ensure the company is in compliance with federal and state employment law carry their responsibilities with Fairness, Integrity & Professional they should Accountability, Development.

1. HRs should clearly communicate expectations through orientations
2. HR should give employees copies or access to COC
3. Supervisors are also responsible for monitoring employees' conduct and for providing honest and timely feedback when an employee fails to meet expectations.

HR RESPONSIBILITIES IN COC VIOLATION

1. To investigate

2. To give quick response
3. To base actions on COC guidelines
4. To give sanctions to the violations

Q no 6

1. Encourage team members to take written notes.
2. Have people write down their questions during the meeting.
3. Break people into groups and have them accomplish small tasks, or make decisions, together.
4. Break the meeting into sections with a different person leading each section or part of the agenda.

Q no 7

Data diddling:

This is called “electronic forgery” in Pakistani legal system and the criminal is awarded punishment up to three years and fine up to two hundred and fifty thousand rupees or both and if the criminal commits this crime in respect to critical infrastructure, he will be imprisoned up to seven years and fine up to five million rupees or both.

Q no 8

Black Hat Hackers:

1. Their intentions are selfish or harmful in nature.
2. Hacking done by black hat hackers is illegal.
3. They infiltrate or control websites, devices, or other systems without permission of the owner/ authorization.
4. Search for the security vulnerabilities to exploit them.
5. Write malware to hack devices, servers, and websites
6. Take advantage of users' lack of awareness about cyber threats to manipulate or defraud them with various phishing techniques.
7. Deploy ransomware and spyware attacks to blackmail individuals/organizations.
8. Steal confidential data that they can use for cybercrime activities or sell to other attackers on the dark web.

White Hat Hackers:

1. Their intentions are noble and often aim to benefit or protect others.
2. Hacking done by white hat hackers is legal.
3. They penetrate the system with the owner's permission. Government agencies and other organizations hire white hats to test the software/devices and carry out non-harmful cyber-attacks to find gaps in their security.
4. They search for security vulnerabilities and offer suggestions and solutions to patch them.
5. Develop security software, tools, and techniques to detect and remove malware.
6. Educate people about cybersecurity threats and risks, as well as ways to mitigate them. Develop tools and contingency plans to help people deal with ransomware and spyware attacks without paying extortion money.

7. Aim to help companies protect sensitive data by strengthening their cyber defenses.

Q no 9

1. Lack of experience.
2. Lack of practice.
3. Lack of related material.
4. Lack of confidence.
5. Hesitation.
6. Ambiguity in the results that you want to conclude.

Q no 10

Hate Speech is a public speech that expresses hate or encourages violence towards a person or group based on something such as race, religion, sexual orientation.

The punishment of Hate Speech according to “Prevention of Electronic Crimes Act”, passed by National Assembly of Pakistan in 2016 is “5 years Imprisonment or 10 million fine or will be both”.