UNIT - V

PROFESSIONAL RESPONSIBILITIES:

Confidentiality and Proprietary Information:

- A hallmark of the professions is the requirement that members of the profession keep certain information of their 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 be 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.

Why must some engineering information be kept 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.

What types of information should be kept confidential?

- Some of these types are very obvious, including test results and data, information about upcoming unreleased products, and designs or formulas for products. Other information that should be kept confidential is not as obvious, including business information such as the number of employees working on a project, the identity of suppliers, marketing strategies, production costs, and production yields.
- Most companies have strict policies regarding the disclosure of business information and require that all employees sign them. Frequently, internal company communications will be labeled as “proprietary.”
- Engineers working for a client are frequently required to sign a nondisclosure agreement. Of course, those engineers working for the government, especially in the defense industry, 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.

- It seems fairly straightforward for engineers to keep information confidential, since it is usually obvious what should be kept confidential and from whom it should be kept. However, as in many of the topics that we discuss in the context of engineering ethics, there are gray areas that must be 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.

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 for 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. The engineering codes are very clear on the need to avoid conflicts of interest like this one.

- There are three types of conflicts of interest that we will consider.
  1. **Actual conflicts of interest:** Such as the one described in the previous paragraph, which compromise objective engineering judgment.
  2. **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 judgment might become conflicted by the desire to maintain the friendship.

  3. 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. can be significant, because the distrust that comes from this situation compromises the engineer’s ability to do this work and future work and calls into question the engineer’s judgment.

Competitive Bidding:

- Competitive bidding was prohibited for several reasons.
- Primarily, bidding was considered to be undignified and not at all in keeping with the image that the engineering profession desired to put forth to the public.
- In addition, there were concerns that if engineers engaged in competitive bidding, it would lead to price being the most significant (or perhaps only) basis for awarding engineering contracts.
- This could lead to engineers cutting corners on design work and could ultimately undermine engineers’ duty to protect the safety and welfare of the public.
- In 1978, the U.S. Supreme Court ruled that professional societies may no longer prohibit competitive bidding.
- This ruling was based on the Sherman Anti-trust Act of 1890 and held that banning bidding was an unfair restraint on free trade.
- This ruling also allowed engineers to advertise, which similarly used to be prohibited by the engineering codes of ethics.
- The rationale behind the Supreme Court ruling was that competitive bidding allows less experienced but competent engineers to compete effectively for work, serves the public interest by helping to keep engineering costs down, and might help promote innovation that leads to better designs and lower costs.
- From the engineer’s perspective, competitive bidding can lead to temptations such as submitting an unrealistically low bid in order to secure work (low-balling).

PROFESSIONAL RIGHTS:

- There are rights that individuals have regardless of the professional status.
- They are:
  1. The right to privacy
  2. The right to participate in activities of one’s own choosing outside of work
  3. The right to reasonably object to company policies without fear of retribution
  4. 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 judgment in discharging one's duties and to exercise this judgment 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 be referred to as the "Right of Conscientious Refusal".
- This is the right to refuse to engage in unethical behavior. Put quite simply, no employer can ask or pressure an employee into doing something that she considers unethical and unacceptable.
- Although this issue is very clear in cases for which an engineer is asked to falsify a test result or fudge on the safety of a product, it is less clear in cases for which the engineer refuses an assignment based on an ethical principle that is not shared by everyone.
- For example, an engineer ought to be allowed to refuse to work on defense projects or environmentally hazardous work if his conscience says that such work is immoral. Employers should be reasonably accommodating of that person's request.

Engineers and the Defense Industry:

- One of the largest employers of engineers worldwide is the defense industry.
- Since fundamentally, weapons are designed for one purpose - to kill human beings- it seems important to look at this type of engineering work in the context of engineering ethics and the rights of engineers.
- An engineer may choose either to work or not to work in defense-related industries and be ethically justified in either position. (even this is also one if the rights of the engineer)
- Many reasonable engineering professionals feel that ethically, they cannot work on designs that will ultimately be used to kill other humans.
- Their remoteness from the killing doesn't change this feeling. Even though they won't push the button or may never actually see the victims of the use of the weapon, they still find it morally unacceptable to work on such systems.
- On the other hand, equally morally responsible engineers find this type of work ethically acceptable.

- They reason that the defense of our nation or other nations from aggression is a legitimate function of our government and is an honorable goal for engineers to contribute to. Both of these positions can be justified using moral theories and ethical problem-solving techniques.

Whistle-Blowing:

- There has been increased attention paid in the last 30 years to whistle-blowing, both in government and in private industry.
- Whistle-blowing is the act by an employee of informing the public or higher management of unethical or illegal behavior 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.

Types of Whistle-Blowing:

1. **Internal whistle-blowing:** Internal whistle-blowing 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 whistle-blowing is kept within the company or organization.
2. **External whistle-blowing:** External whistle-blowing occurs when the employee goes outside the company and reports wrongdoing to newspapers or law-enforcement authorities. Either type of whistle-blowing 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.
   - **Whistle-blowing may be acknowledged or anonymous**

   Anonymous whistle-blowing: Anonymous whistle-blowing 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 or FBI.
   - The employee might also talk to the news media but refuse to let her name be used as the source of the allegations of wrongdoing.

Acknowledged whistle-blowing: Acknowledged whistle-blowing, on the other hand, ccurs when the employee puts his name behind the accusations and is willing to withstand the scrutiny brought on by his accusations.

- Whistle-blowing can be very bad from a corporation's point of view because it can lead to distrust, disharmony, and an inability of employees to work together.

When Should Whistle-Blowing Be Attempted?

1. **Need:**
    - There must be a clear and important harm that can be avoided by blowing the whistle.
    - For example, if an accident occurs at your company, resulting in a spill of a small quantity of a toxic compound into a nearby waterway that is immediately cleaned up, this incident probably does not merit notifying outside authorities.
    - However, if this type of event happens repeatedly and no action is taken to rectify the problem despite repeated attempts by employees to get the problem fixed, then perhaps this situation is serious enough to warrant the extreme measure of whistle-blowing.
2. **Proximity:**
    - The whistle-blower 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.
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.
4. **Last resort**:

- Whistle-blowing 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.

It is important for the whistle-blower to understand his motives before undertaking this step.

Preventing Whistle-Blowing:

- There are four ways in which to solve the whistle-blowing problem within a corporation.
- **First,** there must be a strong corporate ethics culture. This should include a clear commitment to ethical behavior, starting at the highest levels of management, and mandatory ethics training for all employees. All managers must set the tone for the ethical behavior 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 behavior of the company.
- **Fourth,** there should be willingness on the part of management to admit mistakes, publicly if necessary. This attitude will set the stage for ethical behavior by all employees.

COMPUTER ETHICS:

- Computers have rapidly become a ubiquitous tool in engineering and business.
- There are ways in which computers have brought benefits to society.
- Unfortunately, there are also numerous ways in which computers have been misused, leading to serious ethical issues.
- The engineer’s roles as designer, manager, and user of computers bring with them a responsibility to help foster the ethical use of computers. on other issues dealt with in this book.

- For example, many ethical problems associated with computer use relate to unauthorized use of information stored on computer databases and are thus related to the issues of confidentiality and proprietary information.
- Ethical problem-solving techniques used for other engineering ethics problems are equally applicable to computer ethics issues.
- There are two broad categories of computer ethics problems: those in which the computer is used to commit an unethical act, such as the use of a computer to hack into a database and those in which the computer is used as an engineering tool, but is used improperly.

Computers as a Tool for Unethical Behavior:

- Computers can be used to more efficiently steal money from a bank.
- A more traditional bank-robbery method is to put on a mask, hand a note to a bank teller, show your gun, and walk away with some cash.
- Computers can be used to make bank robbery easier to perform and harder to trace.
- The robber simply sits at a computer terminal-perhaps the modern equivalent of a mask-invades the bank's computer system, and directs that some of the bank's assets be placed in a location accessible to him.
- Using a computer, a criminal can also make it difficult for the theft to be detected and traced.
- It is clear that from an ethical standpoint, there is no difference between a bank robbery perpetrated in person and one perpetrated via a computer, although generally the amounts taken in a computer crime far exceed those taken in an armed robbery.
- The difference between these two types of robbery is that the use of the computer makes the crime impersonal.
- The criminal never comes face to face with the victim. In addition, the use of the computer makes it easier to steal from a wide variety of people.
- Computers can be used to steal from an employer: Outsiders can get into a system and steal from an institution such as a bank, or a company can use the computer to steal from its clients and customers.
- In these cases, the computer has only made the theft easier to perpetrate, but does not alter the ethical issues involved.

- Unfortunately, the technology to detect and prevent this type of crime greatly lags behind the computer technology available to commit it.

Computer Design Tools:

- Numerous software packages are available for the design of engineered devices and structures.
- This software includes CAD/CAM, circuit analysis, finite element analysis, structural analysis, and other modeling and analysis programs.
- Software also exists that is designed to aid in the process of testing engineered devices by performing tests, recording data, and presenting data for analysis. These all serve to allow an engineer to work more efficiently and to help take away some of the tedious aspects of an engineer’s work.
- However, the use of this type of software also leads to ethical issues.
- For example, who is responsible when a flaw in software used to design a bridge leads to the failure of the bridge? Is it the fault of the engineer who designed the bridge? Or is it the fault of the company that designed and sold the defective software? Who is at fault when a software package is used for a problem that it isn’t really suited for? What happens when existing software is used on a new and innovative engineering design that software hasn’t yet been developed for? These questions all have the same answer: Software can never be a substitute for good engineering judgment.
- Clearly, the engineer who uses software in the design process is still responsible for the designs that were generated and the testing that was done using a computer.
- Engineers must be careful to make sure that the software is appropriate to the problem being worked on, and should be knowledgeable about the limitations and applicability of a software package.

  Engineers must also keep up to date on any flaws that have been discovered in the software and ensure that the most recent version of the software is being used-software companies make patches and updates available, and engineers must check to make sure they have the most up-to-date version.

Computer Codes of Ethics:

- To aid with decision making regarding these and other computer-related ethics issues, many organizations have developed codes of ethics for computer use.

- The purposes of ethical codes and the way in which codes of ethics function are equally true for codes related to computer use.
- They are guidelines for the ethical use of computing resources, but should not be used as a substitute for sound moral reasoning and judgment.
- They do, however, provide some guidance in the proper use of computer equipment.