Chapter 1

What is Ethics?

Each society forms a set of rules that establishes the boundaries of generally accepted behavior. These rules are often expressed in statements about how people should behave, and they fit together to form the **Moral Code** by which a society lives. The term **Morality** refers to social conventions about right and wrong those are so widely shared that they become the basis for an established consensus.

Definition of Ethics & other terms

- **Ethics**
  is a set of beliefs about right and wrong behavior within a society.
- **Ethical behavior**
  conforms to generally accepted norms, many of which are almost universal.
- **Virtues**
  are habits that incline people to do what is acceptable.
- **Vices**
  are habits of unacceptable behavior.

Difference Between Morals, Ethics, and Laws

- **Morals**
  are one's personal beliefs about right and wrong.
- **Ethics**
  describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs.
- **Law**
  is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, law-making bodies).
- **Legal acts**
  are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do.

Why Fostering Good Business Ethics Is Important

Organizations have at least five good reasons for promoting a work environment in which employees are encouraged to act ethically when making business decisions:

1. Gaining the good will of the community
2. Creating an organization that operates consistently
3. Fostering good business practices
4. Protecting the organization and its employees from legal action
5. Avoiding unfavorable publicity

Characteristics of a successful ethical program

The **Ethics Resource Center** has defined the following characteristics of a successful ethics program:

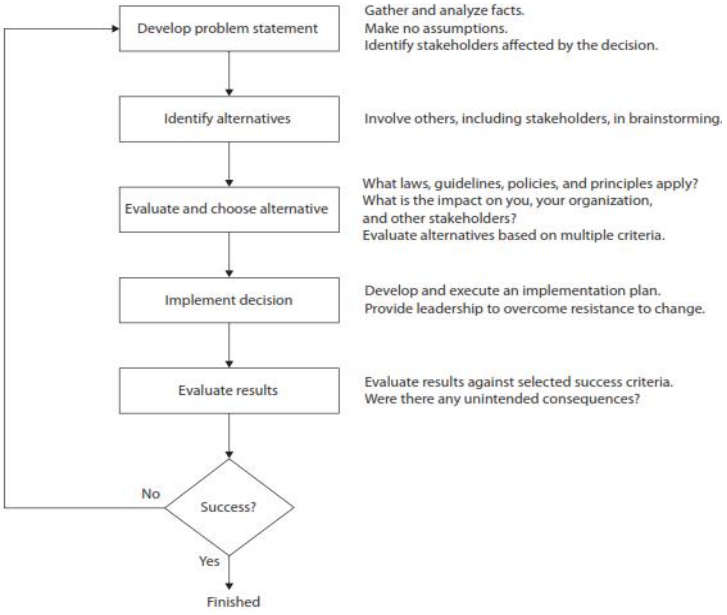
1. Employees are willing to seek advice about ethics issues.
2. Employees feel prepared to handle situations that could lead to misconduct.
3. Employees are rewarded for ethical behavior.
4. The organization does not reward success obtained through questionable means.
5. Employees feel positively about their company.

Improving Corporate Ethics

risk of unethical behavior is increasing, so the improvement of business ethics is becoming more important. following sections explain some of actions corporations can take to improve business ethics.

1. Appointing a Corporate Ethics Officer
2. Ethical Standards Set by Board of Directors
3. Establishing a Corporate Code of Ethics
4. Conducting Social Audits
5. Requiring Employees to Take Ethics Training
6. Including Ethical Criteria in Employee Appraisals

Including Ethical Considerations in Decision Making



Four Common Approaches to Ethical Decision Making

1. **Virtue Ethics Approach**
   The virtue ethics approach to decision making focuses on how you should behave and think about relationships if you are concerned with your daily life in a community.
2. **Utilitarian Approach**
   The utilitarian approach to ethical decision making states that you should choose the action or policy that has the best overall consequences for all people who are directly or indirectly affected.
3. **Fairness Approach**
   The fairness approach focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision. The guiding principle of this approach is to treat all people the same.
4. **Common Good Approach**
   The common good approach to decision making is based on a vision of society as a community whose members work together to achieve a common set of values and goals.

Are IT Workers Professionals

- Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists.
- A partial list of IT specialists includes **programmers**, **systems analysts**, **software engineers**, **database administrators**, **local area network (LAN) administrators**, and **chief information officers (CIOs).**

Relationships Between IT Workers and IT Users

The term **IT user** distinguishes person who uses a hardware or software product from the **IT workers** who develop, install, service, and support the product.
IT users need the product to deliver organizational benefits or to increase their productivity.
IT workers have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs.

Some Important Terminologies

- **Trade Secret** is information, generally unknown to the public, that has economic value and company has taken strong measures to keep confidential.
- **Whistle Blowing** is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.
- **Fraud** is the crime of obtaining goods, services, or property through deception or trickery.
- **Misrepresentation** is the misstatement or incomplete statement of a material fact.
- **Breach of contract** occurs when one party fails to meet the terms of a contract.
- **Bribery** involves providing money, property, or favors to someone in business or government to obtain a business advantage.

Relationships Between IT Workers and Clients

An **IT worker** often provides services to **clients** who either work outside the worker's own organization or are "internal." In relationships between IT workers and clients, each party agrees to provide something of value to the other.

- IT worker provides hardware, software, or services at a certain cost and within a given time frame.
- client provides compensation, access to key contacts, and perhaps a work space.

Typically, the client makes decisions about a project on the basis of information, alternatives, and recommendations provided by the IT worker. The client trusts the IT worker to use his or her expertise and to act in the client's best interests. The IT worker must trust that the client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand the impact of key decisions, and use the information to make wise choices among various alternatives. Thus, the responsibility for decision making is shared between client and IT worker.

Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group and helps promoting:

- Ethical decision making
- High standards of practice and ethical behavior
- Trust and respect from the general public
- Evaluation benchmark

Common Ethical Issues for IT Users

- **Software Piracy**
  Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home.
- **Inappropriate Use of Computing Resources**
  Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games.
- **Inappropriate Sharing of Information**
  Some IT users can share secret and confidential information with an unauthorized party.

Supporting the Ethical Practices of IT Users

- Establishing Guidelines for Use of Company Software
- Defining and Limiting the Appropriate Use of IT Resources
- Structuring Information Systems to Protect Data and Information
- Installing and Maintaining a Corporate Firewall

Chapter 2

Types of Exploits

1. **Virus** is a piece of programming code, usually disguised as something else, which causes a computer to behave in an unexpected and usually undesirable manner.
2. **Worm** is a harmful program that resides in the active memory of the computer and duplicates itself. Worms differ from viruses in that they can propagate without human intervention.
3. **Trojan Horse** is a program in which malicious code is hidden inside a seemingly harmless program.
4. **Botnet** is a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. Botnets are frequently used to distribute spam and malicious code.
5. **Distributed Denial-of-Service (DDoS) Attacks** is one in which a malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks.
6. **Rootkit** is a set of programs that enables its user to gain administrator level access to a computer without the end user's consent or knowledge. Once installed, the attacker can gain full control of the system and even obscure(unclear) the presence of the rootkit from legitimate system administrators. Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration.
7. **Spam** E-mail spam is the abuse of e-mail systems to send unsolicited e-mail to large numbers of people. Most spam is a form of low-cost commercial advertising.
8. **Phishing** is the act of using e-mail fraudulently to try to get the recipient to reveal personal data.
9. **Spear-phishing** is a variation of phishing in which the phisher sends fraudulent e-mails to a certain organization's employees.
10. **phony e-mails** are designed to look like they came from high-level executives within the organization. Employees are again directed to a fake Web site and then asked to enter personal information, such as name, Social Security number, and network passwords.
11. Note:spreading harmful programs or hateful messages, and writing scripts and automated programs that let other people do the same things. ??????????
12. **Insiders** are not necessarily employees; they can also be consultants and contractors. Industrial spies use illegal means to obtain trade secrets from competitors of their sponsor

Types of Perpetrators

Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Trustworthy computing

Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices; this is what organizations worldwide are demanding today. Everyone who provides computing services (software and hardware manufacturers, consultants, programmers) knows that this is a priority for their customers. For example, Microsoft has pledged to deliver on a trustworthy computing initiative designed to improve trust in its software products

Implementing Trustworthy Computing

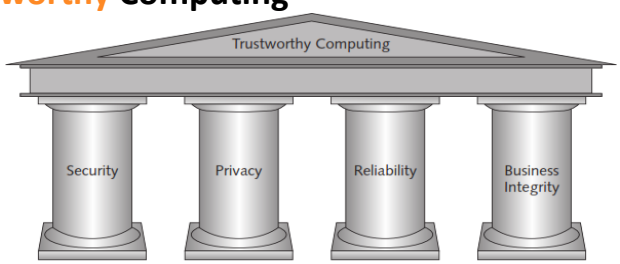


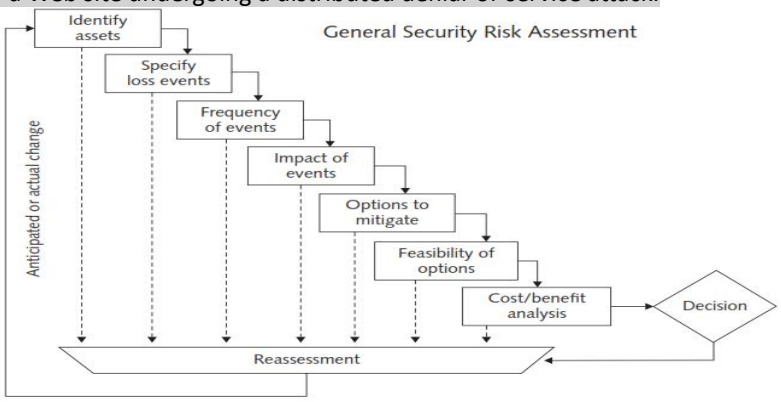
FIGURE 3-3 Microsoft's Four Pillars of Trustworthy Computing

Pillar	Actions taken by Microsoft to support trustworthy computing
Security	Invest in the expertise and technology required to create a trustworthy environment. Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing. Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products. Contribute to standards and policies created by industry organizations and government. Provide users with a sense of control over their personal information.
Reliability	Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) in the event of a disruption, they can be easily restored to a previously known state with no data loss; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) on release, they contain minimal software bugs; and (6) they work as expected or promised.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.

Risk Assessment Process

A risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats. Such threats can prevent an organization from meeting its key business objectives.

The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats. In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives. A loss event is any occurrence that has a negative impact on an asset, such as a computer contracting a virus or a Web site undergoing a distributed denial-of-service attack.



Establishing a Security Policy

A security policy defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements.

A good security policy delineates responsibilities and the behavior expected of members of the organization.

A security policy out-lines what needs to be done but **not** how to do it.

The details of how to accomplish the goals of the policy are provided in separate documents and procedure guidelines.

Educating Employees, Contractors, and Part-Time Workers

Employees, contractors, and part-time workers must be educated about the importance of security so that they will be motivated to understand and follow the security policies.

For example, users must help protect an organization's information systems and data by doing the following:

- Guarding their passwords to protect against unauthorized access to their accounts
- Prohibiting others from using their passwords
- Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
- Reporting all unusual activity to the organization's IT security group

Prevention from threats

Installing a Corporate Firewall: Installation of a corporate firewall is the most common security precaution taken by businesses. A firewall stands guard between an organization's internal network and the Internet, and it limits network access based on the organization's access policy Firewalls can be established through the use of software, hardware, or a combination of both.

- Intrusion Prevention Systems
- Installing Antivirus Software on Personal Computers
- Implementing Safeguards against Attacks by Malicious Insiders
- Conducting Periodic IT Security Audits

Detection.

Even when preventive measures are implemented, no organization is completely secure from a determined attack. organizations should implement detection systems to catch intruders in the act.

An **Intrusion Detection System** is software and/or hardware that monitors system and network resources and activities, and notifies network security personnel when it identifies possible intrusions from outside the organization or misuse from within the organization.

Information Privacy

Information privacy is the combination of

- **communications privacy** (the ability to communicate with others without those communications being monitored by other persons or organizations).
- **data privacy** (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).

Data & Information Privacy Guidelines

Principle	Guideline
Collection limitation	Limit the collection of personal data; all such data must be obtained lawfully and fairly with the subject's consent and knowledge
Data quality	Personal data should be accurate, complete, current, and relevant to the purpose for which it is used
Purpose specification	The purpose for which personal data is collected should be specified and should not be changed
Use limitation	Personal data should not be used beyond the specified purpose without a person's consent or by authority of law
Security safeguards	Personal data should be protected against unauthorized access, modification, or disclosure
Openness principle	Data policies should exist, and a data controller should be identified
Individual participation	People should have the right to review their data, to challenge its correctness, and to have incorrect data changed
Accountability	A data controller should be responsible for ensuring that the above principles are met

Key Privacy Issues

1. **Identity Theft**

   Identity theft occurs when someone steals key pieces of personal information to impersonate a person. This information may include such data as name, address, date of birth, Social Security number, passport number, driver's license number, and mother's maiden name.

   Four approaches are frequently used by identity thieves to capture the personal data of their victims:

   a. Create a data breach to steal thousands, or even millions of personal records;
   b. Purchase personal data from criminals;
   c. Use phishing to entice users to willingly give up personal data; and
   d. Install spyware capable of capturing the keystrokes of victims.

2. **Consumer Profiling**

   - Companies openly collect personal information about Internet users when they register at Web sites, complete surveys, fill out forms, or enter contests online.
   - Many companies also obtain information about Web surfers using cookies, text files that a Web site can download to visitors' hard drives so that it can identify visitors on subsequent visits.
   - Companies also use tracking software to allow their Web sites to analyze browsing habits and deduce personal interests and preferences.

3. **Treating Consumer Data Responsibly**

   The most widely accepted approach to treating consumer data responsibly is for a company to adopt the Fair Information Practices and the privacy guidelines.

   Under these guidelines, an organization collects only personal information that is necessary to deliver its product or service.

4. **Workplace Monitoring**

   Many organizations have developed a policy on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or expose the employer to harassment lawsuits.

5. **Advanced Surveillance Technology**

   advances in information technology such as surveillance cameras, facial recognition software, and satellite-based systems that can pinpoint a person's physical location provide exciting new data-gathering capabilities.

Chapter 3

Key Ethical Issues for Organizations

1. **Non-Traditional Workers**
2. **Whistle-blowing**
3. **Green Computing**
4. **ICT Code to Address Ethical Issues**

The Need for Non-Traditional Workers

- **Contingent Workers**
  Typically, these workers join a team of full-time employees and other contingent workers for the life of the project and then move on to their next assignment.
  The Bureau of Labor Statistics defines contingent work as a job situation in which an individual does not have an explicit or implicit contract for long-term employment.
  // A firm is likely to use contingent IT workers if it experiences pronounced fluctuations in its technical staffing needs.
- **Advantages**
  - When a firm employs a contingent worker, it does not usually have to provide benefits such as insurance, paid time off, and contributions to a retirement plan.
  - A company can easily adjust the number of contingent workers it uses to meet its business needs, and can release contingent workers when they are no longer needed.
- **Disadvantages**
  - One downside to using contingent workers is that they may not feel a strong connection to the company for which they are working.
  - This can result in a low commitment to the company and its projects, along with a high turnover rate.

Outsourcing

Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.
Outsourcing is another approach to meeting staffing needs.
A company may contract with an organization to provide such services as operating a data center, supporting a telecommunications network, or staffing a computer help desk.

Offshore Outsourcing

Offshore Outsourcing is a form of outsourcing in which the services are provided by an organization whose employees are in a foreign country.
However, IT professionals can do much of their work anywhere—on company's premises or thousands of miles away in a foreign country.

Whistle-Blowing

- **Whistle-blowing** is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.
- In some cases, whistle-blowers are employees who act as informants on their company, revealing information to enrich themselves or to gain revenge for a perceived wrong.
- A whistle-blower usually has personal knowledge of what is happening inside the offending organization because of his or her role as an employee of the organization.

Green Computing

- Green computing is a term applied to a variety of efforts directed toward the efficient design, manufacture, operation, and disposal of IT-related products, including personal computers, laptops, servers, printers, and printer supplies.
- Many computer manufacturers today are talking about building a "green PC," by which they usually mean one that uses less electricity to run than the standard computer; thus, its carbon footprint on the planet is smaller.

ICT Industry Code of Conduct

The Electronic Industry Citizenship Coalition (EICC) was established to promote a common code of conduct for the electronics and information and communications technology (ICT) industry.

The following are the five areas **of social responsibility** and guiding principles covered by the code:

1. **Labor**

   Participants are committed to uphold the human rights of workers, and to treat them with dignity and respect as understood by the international community.

2. **Health and Safety**

   A safe work environment improves product quality and worker morale, with ongoing worker input key to safety. // ↓تحت الأصلي. عندي من القصير التعريف

   Participants recognize that in addition to minimizing the incidence of work-related injury and illness, a safe and healthy work environment enhances the quality of products and services, consistency of production and worker retention and morale. Participants also recognize that on-going worker input and education is essential to identifying and solving health and safety issues in the workplace.

3. **Environment**

   Environmental responsibility ensures quality products and less harm to the community. // ↓تحت الأصلي. عندي من القصير التعريف

   Participants recognize that environmental responsibility is integral to producing world class products. In manufacturing operations, adverse effects on the community, environment, and natural resources are to be minimized while safeguarding the health and safety of the public.

4. **Management System**

   Participants shall adopt or establish a management system whose scope is related to the content of this Code.

   The management system shall be designed to ensure

   a) Compliance with applicable laws, regulations and customer requirements related to the participant's operations and products
   b) Conformance with this Code
   c) Identification and mitigation of operational risks related to this Code. It should also facilitate continual improvement.

5. **Ethics**

   To meet social responsibilities and to achieve success in the marketplace, participants and their agents are to uphold the highest standards of ethics including: business integrity; no improper advantage; disclosure of information; intellectual property; fair business, advertising, and competition; and protection of identity.

Tele-work

Tele-work (or Telecommuting) is a work arrangement in which an employee works away from the office at home, at a client's office, in a hotel, anywhere.

Note// In Tele-work, an employee uses various forms of electronic communication, including e-mail, audio conferencing, video conferencing, and instant messaging.

Telework for Employees	
Advantages	**Disadvantages**
People with disabilities who otherwise find public transportation and office accommodations a barrier to work may now be able to join the workforce.	Some employees are unable to be productive workers away from the office.
Teleworkers avoid long, stressful commutes and gain time for additional work or personal activities.	Teleworkers may suffer from isolation and may not really feel "part of the team."
Telework minimizes the need for employees to take time off to stay home to care for a sick family member.	Workers who are out of sight also tend to be out of mind. The contributions of teleworkers may not be fully recognized and credited.
Teleworkers have an opportunity to experience an improved work/family balance.	Teleworkers must guard from working too many hours per day because work is always there.
Telework reduces ad hoc work requests and disruptions from fellow workers.	The cost of the necessary equipment and communication services can be considerable if the organization does not cover these.

Telework for Organizations	
Advantages	**Disadvantages**
As more employees telework, there is less need for office and parking space; this can lead to lower costs.	Allowing teleworkers to access organizational data and systems from remote sites creates security issues.
Allowing employees to telework can improve morale and reduce turnover.	Informal, spontaneous meetings become more difficult if not impossible.
Telework allows for the continuity of business operations in the event of a local or national disaster and supports national pandemic- preparedness planning.	Managers may have a harder time monitoring the quality and quantity of the work performed by teleworkers, wondering, for instance, if they really "put in a full day."
The opportunity to telework can be seen as an additional perk that can help in recruiting.	Increased planning is required by managers to accommodate and include teleworkers.
There may be an actual gain in worker productivity.	There are additional costs associated with providing equipment, services, and support for people who work away from the office.
Telework can decrease an organization's carbon footprint by reducing daily commuting.	Telework increases the potential for lost or stolen equipment.

The Digital Divide

Another indicator of the standard of living is the availability of technology.
The **Digital Divide** is a term used to describe the gulf between those who do and those who don't have access to modern information and communications technology such as cell phones, personal computers, and the Internet.
The digital divide exists not only between more and less developed countries but also within countries—among age groups, economic classes, and people who live in cities versus those in rural areas.

E-Rate Program

The **Education Rate (E-Rate)** program was created through the Telecommunications Act of 1996.
One of E-Rate's goals is to help schools and libraries obtain access to state-of-the-art services and technologies at discounted rates.
The program's discounts range from 20 percent to 90 percent for eligible telecommunications services, depending on location (urban or rural) and economic need.

Electronic Health Records

An **electronic health record (EHR)** is a summary of health information generated by each patient encounters in any healthcare delivery setting.
An EHR includes patient demographics, medical history, immunization records, laboratory data, problems, progress notes, medications, vital signs, and radiology reports.
Note// **Healthcare professionals** can use an EHR to generate a complete electronic record of a clinical patient encounter.

Telemedicine

Telemedicine employs modern telecommunications and information technologies to provide medical care to people who live far away from healthcare providers.

There are two basic forms of telemedicine:

1. **Store-and-Forward Telemedicine**
   involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.
2. **Live Telemedicine**
   requires the presence of patients and healthcare providers at the same time and often involves a video conference link between the two sites.

Chapter 4

Intellectual Property

- Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct, and owned or created by a single person or group.
- Intellectual property is protected through **copyright**, **patent**, and **trade secret** laws.

Copyrights @

A copyright is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work.

Copyright infringement

Copyright infringement is a violation of the rights secured by the owner of a copyright.
Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission.

Eligible Works

The types of work that can be copyrighted include architecture, art, audio-visual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works.

Fair Use Doctrine

The fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances.

Software Copyright Protection

To prove infringement, the copyright holder must show a striking resemblance between its software and the new software that could be explained only by copying.

Patents.

A patent is a grant of a property right issued by the United States Patent and Trademark Office (USPTO) to an inventor.

A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators.

Patent infringement

Patent infringement, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another's patent.

Unlike copyright infringement, there is **no** specified **limit** to the monetary penalty if patent infringement is found.

Software Patents

A software patent claims as its invention some feature or process embodied in instructions executed by a computer.

Software Cross-Licensing Agreements

Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements.

Trade Secrets

A trade secret is defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.

Key Intellectual Property Issues

1. **Plagiarism** is the act of stealing someone's ideas or words and passing them off as one's own.
2. **Reverse Engineering** is the process of taking something apart in order to understand it.
3. **Open-Source Code** is any program whose source code is made available for use or modification, as users or other developers see fit.
4. **Competitive Intelligence** is legally obtained information that is gathered to help a company gain an advantage over its rivals.
5. **Cyber-Squatting** Cyber-squatters registered domain names for famous trademarks or company names to which they had no connection, with the hope that the trademark's owner would eventually buy the domain name for a large sum of money.

   A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.

Chapter 5

Why High-quality software systems are easy to learn and use?

because they perform quickly and efficiently; they meet their users' needs; and they operate safely and reliably so that system downtime is kept to a minimum.
Such software has long been required to support the elds of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration.
Note// the demand for high-quality software is increasing.

- **Software Defect** is any error that, if not removed, could cause a software system to fail to meet its users' needs.
- **Software Quality** is the degree to which a software product meets the needs of its users.
- **Quality Management** focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.
- **The objective** of Quality Management is to help developers deliver high-quality systems that meet the needs of their users.

The Importance of Software Quality

- The accurate, thorough, and timely processing of business transactions is a key requirement for safety critical systems.
- A software defect can be devastating, resulting in lost customers and reduced revenue.

Key Issues in Software Development

- **Software Defect** can be devastating, resulting in lost customers and reduced revenue.
- **Ethical Decisions** involving a trade-off if one must be considered between quality and such factors as cost, ease of use, and time to market require extremely serious examination.

Development of Safety-Critical Systems

- A safety-critical system is one whose failure may cause injury or death.
- The safe operation of safety-critical systems relies on the flawless performance of software;
- such systems control automobiles' antilock brakes, nuclear power plant reactors, airplane navigation, roller coasters, elevators, and numerous medical devices, to name just a few.
- The process of building software for such systems requires highly trained professionals, formal and rigorous methods, and state-of-the-art tools.

Points to consider while Developing Safety-Critical Systems

1. **International Standards** When developing safety-critical systems, a key assumption must be that safety will not automatically result from following an organization's standard development methodology.
2. **Rigorous Software Development** Process Safety-critical software must go through a much more rigorous and time-consuming development process than other kinds of software.
3. **Project Safety Engineer** The key to ensuring that these additional tasks are completed is to appoint a project safety engineer, who has explicit responsibility for the system's safety. The safety engineer uses a logging and monitoring system to track hazards from a project's start to its finish.
4. **Sufficient Testing** Another key issue is deciding when the QA staff has performed sufficient testing. How much testing is enough when you are building a product whose failure could cause loss of human life?
5. **Formal Risk Analysis** When designing, building, and operating a safety-critical system, a great deal of effort must be put into considering what can go wrong.
6. **Redundancy** Another key element of safety-critical systems is redundancy, the provision of multiple interchangeable components to perform a single function in order to cope with failures and errors.
7. **Human Interface** One of the most important and difficult areas of safety-critical system design is the human interface.

Quality Management Standards

- The International Organization for Standardization (ISO), founded in 1947, is a worldwide federation of national standards bodies from 161 countries.
- The ISO issued its 9000 series of business management standards in 1988. The ISO 9000 standard serves as a guide to quality products, services, and management.
- These standards require organizations to develop formal quality-management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.

To obtain this coveted certificate, an organization must submit to an examination by an external assessor and fulfill the following requirements:

1. Have written procedures for all processes
2. Follow those procedures
3. Prove to an auditor that it has fulfilled the first two

requirements; this proof can require observation of actual work practices and interviews with customers, suppliers, and employees.

The various ISO 9000 series of standards address the following software-related activities:

1. **ISO 9001**: Design, development, production, installation, servicing
2. **ISO 9002**: Production, installation, servicing
3. **ISO 9003**: Inspection and testing
4. **ISO 9000-3**: Development, supply, and maintenance of software
5. **ISO 9004**: Quality management and quality systems elements

CH-3

Short Questions

1) List down the key ethical issues for the organization.
2) Write down two advantages and two disadvantages for Contingent works.
3) Differentiate between Outsourcing and Offshore Outsourcing.
4) What is whistle blowing?
5) What is green computing?
6) Write down any three advantages and disadvantages for teleworking for Employees.
7) Define Digital divide.
8) What is Electronic Health Record (HER)?

Long Questions

1) Explain whistle – blowing with the help of example.
2) Explain Green Computing with its goals.
3) List down the four areas of social responsibility and guiding principles covered by the ICT industry code of conduct and explain any two.
4) Explain Telemedicine and its type.

CH-4

براءات الاختراع

Short Questions

1) What is eligible work?
2) What is copyright? How does copyright infringement occur?
3) What is patent? How does patent infringement occur?
4) Differentiate between copyright infringement and patent infringement.
5) What is *Fair Use Doctrine?*
6) What is Trade Secret?
7) List down the key Intellectual property issues.

Long Questions

1) What is Intellectual property? Explain any four key intellectual property issues.
2) How intellectual property is protected? Explain
3) Write Comprehensive notes on Key intellectual property issues.

CH-5

Short Questions

1) Why high quality software systems are easy to learn and use?
2) Why the demand for high quality software is increasing?
3) What is Safety critical system?
4) Define Reverse Engineering.
5) How do we define formal risk analysis?
6) List down the three requirements to obtain the coveted certificate for ISO 9000 standard serve as a guide to quality products, services and management.
7) List down ISO 9001,ISO 9002 and 9003 standards with their related activities .

Long Questions

1) Explain any five points that are considered while developing safety critical Systems.
2) Explain quality management standard with the help of example.
3) List down ISO 9000 series of standard with their related activities.