* Abbreviations

1) CSR - Corporate Social Responsibility
2) BYOD - Bring Your Own Device
3)

* Computer Incidents

- Computer Incidents refer to events or occurances that compromises the security, integrity or availability of computer systems, networks, or data.

- Computer incidents can have significant consequences, such as financial losses, reputational damage, and distruption of operations. Organizations need to be vigiliant and implement robust cyber-security measures to prevent and mitigate these incidents effectively.

* Types of Exploits

1) Malware Infections
- Malicious software like viruses, worms or ransomware can infiltrate computers causing data theft, system damage or financial loss

2) Data Breaches
- Unauthorized access to sensetive information through hacking or social engineering can lead to the exposure of personal, financial or proprietary data.

3) Denial of Service (DoS) Attacks
These aim to distrupt systems or networks by flooding them with excessive traffic, rendering them inaccessible to legitimate users.

4) Unautorized Access
Intruders exploit vulnerabilities or weak passwords to gain unauthorized entry into computer systems or networks.

5) Insider Threats : Trusted individuals misuse their privilages to steal data or introduce vulnerabilities, intentionally or unintentionally.

6) Data loss : Accidental deletion, corruption or loss of data can occur due to various factors including hardware failures, software bugs or human error.

7) Ransomware : Malware encrypts data, demanding payment for decryption keys, posing a serious threat to organizations and individuals.

8) Advanced Persistant Threats (APTs) : Sophisticated, long-term cyber attacks conducted by well-funded adversaries, often targeting specific entities like government agencies or corporations.

* Computer Security Triad
(Confidentiality, Integrity, Availability)

1) Confidentiality

- No Unautorized person

- Methods that breach Confidentiality are Social engineering, Password cracking, Phishing scams, Malware attacks, Unsecured networks and systems, Insider threat

- Tools available to achieve confidentiality are veracrypt, Truecrypt, Bitlocker, xCrypt, etc

2) Integrity

- No modification of data

- Guarentees that data remain accurate, complete and unaltered during transmission or storage.

- Methods that breach integrity are SQL Injection, Malware attacks, man-in-the-middle attacks.

- Techniques such as data validation, checksums, digital signatures, and access controls help maintain data integrity and prevent unauthorized access or modifications

3) Availability

- No data inaccessibility

- Ensures that data and systems are accessible and usable when needed by authorized users

- Methods that breach Availability are DDoS attacks, Malware attacks, Power outages & failures.

- Implementing measures : data redundency, fault tolerance, backups and disaster recovery plans

* Implementing CIA at the Organizational level

Implementing the CIA triad at the organizational level involves integrating these principles into various aspects of information security management

1) Risk Assessment

Identify, prioritize, and mitigate potential threats and vulnerabilities to data and systems

2) Security Strategy

Align security goals with business objectives and allocate resources effectively.

3) Disaster Recovery

Develop plans to ensure business continuity in the event of disruptive incidents or disasters

4) Security Policies

Establish and enforce policies and procedures to govern access, data protection, and incident response.

5) Security Audit

Regularly assess and update security controls to address gaps and ensure compliance with regulations.

6) Regulatory Compliance

Stay informed about industry regulations and standards, and maintain compliance accordingly.

7) Security Dashboard

Monitor key security metrics and incidents to track performance and inform decision making

* Implementing CIA at the Network level

At the network level, implementing the CIA triad involves integrating following security measures:-

1) Authentication Methods

Implementing strong authentication methods like multi-factor authentication (MFA) or biometric authentication to verify the identity of users accessing the network. This ensures that only authorized individuals can gain access to sensetive information.

2) Firewall

Deploy firewall to monitor and control incoming and outgoing network traffic. Firewalls use predefined rules to filter traffic, allowing only authorized communication and preventing unauthorized access and maintain data integrity.

3) Routers

Configure routers with access control lists (ACLs) to filter and restrict traffic based on predefined rules. This helps ensure that only legitimate traffic is allowed, protecting against unauthorised access.

4) Encryption

Utilize encryption protocols such as SSL/TLS to encrypt data in transit between network devices and endpoints. Encryption protects the confidentiality of data

5) Proxy Servers and VPNs

Employ proxy servers and Virtual Private Networks (VPNs) to provide secure remote access to network resources for authorised users. This ensures the availability of critical servers and data from anywhere while maintaining confidentiality and integrity.

* Implementing CIA at the Application level

At the application level, implementing the CIA triad involves incorporating various security measures.

1) Authentication Methods

Implement robust authentication methods such as username/password combinations, multi-factor authentication (MFA), or biometric authentication. This ensures that only authorised users can access the application and its data enhancing confidentiality.

2) User Roles and Accounts

Define user roles and access levels within the application based on the principal of least privilage. Assign appropivate permissions to each user roles to restrict access to sensetive data and functionalities, thereby protecting confidentiality and integrity.

3) Data Encryption

Utilize encryption techniques to protect sensetive data stored within the application or transmitted over networks. Implement encryption algorithms such as AES (Advanced Encryption Standard) to encrypt data at rest and in transit, safeguarding confidentiality and integrity

*Implementing CIA at the End-User Level

At the end-user level, implementing the CIA triad involves empowering users with knowledge and tools.

1) Security Education

- Provide comprehensive security awareness training to end users, educating them about common threats, best practices, and the importance of security measures.

- Teach users how to recognize phishing emails, social engineering tactics, and other forms of cyber threats to prevent unauthorized access and data breaches.

2) Authentication Methods

- Implement strong authentication methods for user access, such as complex passwords, multi-factor authentication (MFA) or biometric authentication.

3) Antivirus Software

- Deploy and regularly update antivirus software on end-user devices to detect and prevent malware infections, including viruses, worms, Trojens, etc.

4) Data Encryption

- Encourage the use of encryption tools and techniques to protect sensetive data stored on end-user devices or transmitted over networks.

- Provide guidence on encrypting sensetive files and communications, as well as using encrypted messaging apps or email services to ensure the confidentiality of data.

* Response to Cyber Attack

Responding effectively to cyber attacks requires a well-defined incident response plan and a coordinated effort across multiple fronts.

1) Incident Notification

- Internal Notification: Alert internal incident response team and relevant stakeholders immediately

- External Notification: Comply with legal and regulatory requirements for data breach notification

- Clear Communication: Provide concise updates on the incident's nature, impact and response efforts

- Support and Guidance: Offer assistance and resources to affected parties

- Transparency: Maintain openness and accountability throughout the response process.

2) Protection of Evidence and activity logs.

- Immediate Preservation: Securely store all relevant evidance, including logs, network traffic data and system snapshots, to prevent tempering or deletion.

- Chain of custody: Maintain a clear chain of custody for evidance, documenting who accessed or handled it to ensure its integrity for legal proceedings.

- Access controls: Limit access to evidance and activity logs to authorised personnel only to prevent tampering.

- Documentation: Thoroughly document all actions taken to preserve evidance and activity logs including timestamps, descriptions of activities.

3) Incident Containment

- Isolation: Quickly isolate affected systems or networks to prevent further spread of the attacks and minimize damage to other assets.

- Segmentation: Segment networks and systems to contain the attack within specific areas, limiting its reach and impact on critical infrastructure.

- Blocking: Block malicious IP addresses, domain names or URLs associated with the attack to prevent communication with command and control servers or malicious actors.

4) Eradication

- Malware Removal: Use antivirus software, malware removal tools, or specialized forensic analysis techniques to identify and remove malicious software

- Patch and Update: Apply security patches and updates to vulnerable systems to eliminate known vulnerabilities

- Password reset: Reset passwords for compromised user accounts and system accounts to prevent unauthorized access by the attacker.

- System Reimaging: Reimage or rebuild compromised systems from clean backups or known-good images to ensure that all traces of malicious activity are eradicated.

5) Incident follow up using MSSP
(Managed Security Service Provider)

- Incident Reporting: Immediately report the incident to the MSSP, providing all relevant details, such as nature of incident, affected systems.

- Incident Analysis: The MSSP will conduct a through analysis of the incident data, including logs, alerts and network traffic to understand the scope and impact.

- Continuous monitoring: Utilize the MSSP's monitoring capabilities to conduct & track the incident's progress and monitor for any signs of recurrence of additional threats

* Software Quality

Software quality refers to the degree to which a software product meets specified requirements and satisfies customer needs and expectations. It encompasses various attributes such as functionality, reliability, usability, efficiency, maintainability and portability.

The various Importance of Quality Software :

1) Customer Satisfaction

High Quality Software ensures that customers receive products that meet their expectations, leading to satisfaction and loyalty.

2) Competitive Advantage

In today's competitive market, quality can be a key difference maker. Software that is reliable, easy to use, and bug-free can give a company a significant edge over its competitors.

3) Cost Savings

Investing in quality early in software development can save money in the long run. High quality software typically requires fewer resources for maintenance, support and bug fixes, reducing overall development costs.

4) Reduced Risk

Poor-quality software can lead to various risks, including security breaches, data loss, system failures, damage to company's reputation. Investing in quality software helps mitigate these risks and ensures the stability and security of the software.

5) Brand Reputation

The quality of company's software reflects its overall brand reputation. Consistently delivering high-quality products reinforces a positive brand image and strengthens the company's position in the market.

* Strategies for Developing Quality Software

1) Define Clear Requirements

Start by clearly defining and documenting the requirements of the software. Involve stakeholders early in the praess to ensure that their needs and expectations are understood and captured accurately.

2) Use Agile Methodologies

Agile methodologies, such as scrum or kanban, promote iterative development, frequent testing, and continuous feedback. This allows for early detection and correction of issues, leading to higher-quality software.

3) Implement Test-Driven Development (TDD)

TDD involves writing tests before writing the actual code. This helps ensure that the code meets the specified requirements and involves test coverage. Developer can use automated testing framework to run tests frequently.

4) Code Reviews

Conduct regular code reviews to identify potential issues, involve code quality, and promote knowledge sharing among team members. Code reviews help catch bugs, ensure adherence to coding standards and improve overall code maintainability.

5) Continuous Integration and Continuous Deployment (CI/CD)

Implement CI/CD pipelines to automate the build test, and deployment processes. This allows for rapid feedback on code changes and helps ensure that only high quality code is deployed to production.

6) User Acceptance Testing (UAT)

Involve end-users in the testing process through UAT to validate that the software meets their needs and expectations. User feedback is invaluable for identifying usability issues and making necessary improvements.

*Privacy Protection and the law

- Government and organizations gather, store, analyze and report the information of the people because they can use it to make better decisions.

- Many people object to the data collection policies of the governments and the businesses on the grounds that they strip (remove) individuals of the power to control their own personal information.

- For those people, the existing privacy laws and practices fails to provide adequate protection; rather it causes confusion that promotes distrust and skepticism (doubt as to the truth of something), which are further fueled by the disclosure of threats to privacy.

* Information Privacy

A broad definition of the right of privacy is "the right to be left alone - the most comprehensive of rights, and the most valued by a free people."

Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and 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 their use).

* Key Privacy and Anonymity Issues

1) Consumer Profiling

- Companies openly collect personal data and information about users when they register at websites, complete surveys, fill out forms, follow them on social media or enter contests online.

- Companies use tracking software to allow their websites to analyze browsing habits and deduce personal interests and preferences.

- The operator can use these data to initiate contact or sell it to other organizations with which they have marketing agreements.

21 Identity Theft

Identity Theft is the theft of personal information, which is then used without the owner's permission.

Thieves may use a customer's credit card number to charge items to that person's account, use identification information to apply for a new credit card or a loan in a consumer's name, or use a consumer's name and social security number to obtain government benefits.

- Thieves also often sell personal identification information on the black market.

3) Electronic Discovery

Electronic Discovery is the part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.

Electronic Discovery (e-discovery) is the collection preparation, review and production of electronically stored information for use in criminal and civil actions and proceedings.

Electronically stored Information (ESI) includes any form of digital information, including emails, drawings, graphs, web pages, photographs, word processing files, sound recordings and databases stored on any form of magnetic storage device, including hard drives, CDs and flash drives.

4) Workplace Monitoring.

* Cyberloafing

Cyberloafing is defined as using the Internet for purposes unrelated to work such as posting to facebook, sending personal emails or Instant messages, or shopping online.

Some surveys reveal that the least productive workers cyberloaf more than 60% of their time at work.

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

* Advanced Surveillance Technology

A number of advances in Information technologies - such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location - provide amazing new data-gathering capabilities.

* Camera Surveillance

Surveillance cameras are used in major cities around the world in any effort to deter crime and terrorist activities.

Critics believe that such critical observation or examination is an violation of civil liberties and are concerned about the cost of the equipment and people required to monitor the video feeds.

Stalking Apps

Technology has made it easy for a person to track the whereabouts of someone else at all times, without ever having to follow the person.

A built-in microphone can be activated remotely to use as a listening device even when phone is turned off.

All information gathered from such apps can be sent to the user's email account to be accessed live or at a later time.

Some of the most popular spy software includes Mobile Spy, ePhoneTracker, FlexiSPY, and Mobile Nanny.

* Defamation

The right to freedom of expression is restricted when the expressions, whether spoken or written, are untrue and cause harm to another person.

Making an oral or a written statement of alleged fact that is false and that harms another person is defamation.

Because defamation is defined as an untrue statement of fact, truth is an absolute defense against a charge of defamation.

Although people have the right to express opinions, they must exercise care in their online communications to avoid possible charges of defamation.

* Freedom of Expression : Key Issues

- Controlling access to information on the Internet
- Internet filtering
- Internet Censorship

- Doxxing
  - Involves doing research on the Internet to obtain someone's private personal information

- Hate Speech
- Fake News

* Social Networking Ethical Issues

- Cyberabuse, Cyber harassment and Cyberstalking
- Encounter with social Predators
- Uploading of Inappropriate Material

* 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 a group.

It is protected through copyright, patent and trade secret laws.

Copyright law protects authorized works, such as books, film and music.

Patent law protects inventions and

Trade secret law helps safeguard information that is critical to an organization's success.

*Copyrights

Copyright protection is established through The Copyright Act, 2059 (2002) and amended in 2063.

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 protection is granted to the creators of "original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated either directly or with the aid of a machine or device".

* Copyright term

The copyright Act 2059 of Nepal defines that the economic and moral rights available to the author shall be protected throughout the life of the author and in the case of his/her death until fifty years completed from the year of death.

* Eligible work

The types of work that can be copyrighted include architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pictures, sculptures, sound recordings and other intellictual works.

- Copyright law has proven to be extremely flexible in covering new technologies: thus software, video games, multimedia works and web pages can all be protected. However, evaluating the originality of the

work is not always a straightforward process and disagreements of whether or not as work is original sometimes lead to litigation.

* Economic Right

As per the Copyright Act 2059 of Nepal, only the author or the owner of copyright shall have the exclusive right to carry out the following acts in respect of the work:

i) To reproduce the work.
ii) To translate the work.
iii) To revise or amend the work
iv) To make arrangement and other transformation of the work
v) To have public exhibition of the original or copy of the work.

* Fair Use Doctrine

The chapter 4 of Copyright Act 2059 of Nepal specifies a certain circumstances where the copyrighted materials can be used without authorization.

Section 16: Reproduction allowed for personal purpose - no authorization shall be required from the author of the copyright owner to reproduce some portion of any published work for personal use.

Section 17: Citation allowed

Section 18: Reproduction allowed for learning and learning

Section 20: Reproduction broadcast or other communication allowed for purposes of information to the general public

* Infringement of Protected Right and Punishment:

- To reproduce copies of work or sound recording and sell and distribute them to publicly communicate or rent them with commercial or any motive with or without deriving economic benefits without authorization of the author.

- To make work of another subject or nature by changing the form and language of a work belonging to another person with a motive of delivering economic benefit

- To import, produce or rent any equipment or device prepared with intention of circumventing any device designed to discourage the unauthorized reproduction.

* Patents

A patent is a grant of a property right to an inventor. A patent permits its owner to exclude the public from making, using or selling a protected invention, as it allows for legal action against violators.

Unlike a copyright, a patent prevents independent creation as well as copying. Even if someone else invents the same item independently and with no prior knowledge of patent holder's invention, the second inventor is excluded from using the patented device without permission of the original patent holder.

A person desirous of obtaining right over any patent shall register such patent in his/her name under this act.

No one shall copy or use or cause to use in the name of other without transforming the ownership.

*Trade Secret

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.

Trade secret laws protects only against the misappropriation of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn't prevent someone from using the same idea if it was developed independently.

* Employees and trade secrets

Employees are the greatest threat to the loss of company trade secrets - they might accidently disclose trade secrets or steal them for monetary gain. Organization must educate employees about the importance of mantaining the secrecy of the corporate information.

Trade secret information should be labeled clearly as confidential and should only be accessible by a limited number of people.

Most organizations have strict policies regarding nondisclosure of corporate information.

* Intellictual Property Issues

- Plagiarism
- Reverse Engineering
- Open Source Code

- Competitive Intelligence

- Trademark Infringement

* Ethics

- Ethics is a code of behaviour that is defined by the group to which an individual belongs.

- Ethical behaviour are the norms, which may change over time to meet the evolving needs of the society or the group of people who share same laws, traditions, and values that provide structure to enable them to live in an organized manner.

* Morals

- Morals are the personal principles upon which an individual bases his or her decisions about what is right and wrong.

- Your moral principles are statements of what you believe to be rules of right conduct.

* Ethics in the business world

The system of ethical beliefs that guides the values, behaviours, and decisions of a business organization and the individuals within that organization is known as business ethics.

Unethical behaviour in the business world can lead to serious negative consequences for both organizations and individuals.

Ethics and moral principles are vital attributes for any business to earn and sustain the trust of customers for longetivity, sustain undisputed and unquestioned business for ever, and enjoy long term success in term of revenue and reputation

* Features of Business Ethics

1) Integrity

Business ethics emphasize honesty, truthfulness and adherence to moral principles in all business dealings.

2) Fairness

fairness entails treating all individuals and groups fairly and impartially, without discrimination or favoritism. This applies to employees, customers, suppliers, and other stakeholders.

3) Respect for Stakeholders

Business ethics acknowledge the interests and rights of all stakeholders, including employees, customers, shareholders, suppliers, and the community.

4) Transparency

Transparency involves openness and clarity in communication and decision making proiers.

5) Accountability

Ethical businesses take responsibility for their actions and decisions. This includes holding individuals and organizations accountable for unethical behaviour

6) Long-term Orientation

Business ethics prioize long-term sustainability over short-term gains. Ethical businesses recognize that ethical behavior is not only morally right but also beneficial for long-term success and reputation.

* Some unethical practices devastating business ethics.

1) Economic and financial Scandals

- Manipulation of financial & business data
- Illegal usage of price sensitive info of business
- Bribery to certain internal and external stakeholders
- Unauthorized related party transactions.

2) Intellictual Property Rights (IPR)

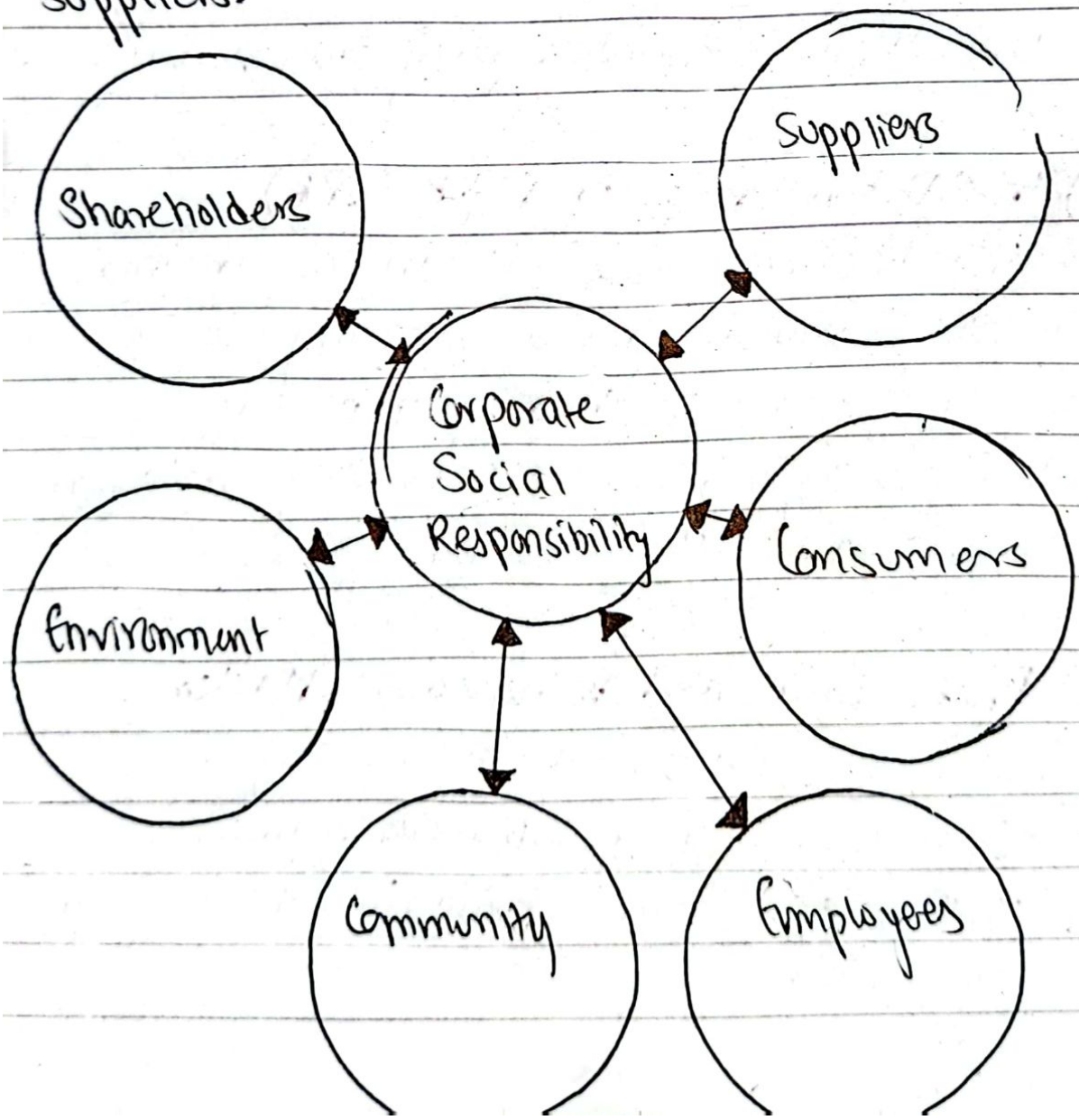
- Unauthorized usage of IPR of another person/company by a company for its benefit or any third party benefit.
- Usage of product or service in violation or violation of third party IPR.

3) Professional and Behavioural Matters

- Sexual harassment
- Discrimination in job/work allocation
- Unfair terms and conditions of the employment agreement.

* Corporate Social Responsibility (CSR)

Corporate Social Responsibility (CSR) is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment and suppliers.



- An organization's approach to CSR can encompass a wide variety of tactics - from donating a portion of net profit to charity to implementing more sustainable business operations or encouraging employee education through tuition reimbursement.

- Setting CSR goals encourages an organization to achieve higher moral and ethical standards.

- **Supply Chain Sustainability** is a component of CSR that focuses on developing and maintaining a supply chain the needs of the present without compromising the ability of future generations to meet their needs.

*Business Benefits of CSR

Corporate Social Responsibility (CSR) offers numerous benefits to businesses, both tangible and intangible. Here are some of the key benefits.

1) Enhanced Brand Reputation

Engaging in CSR activities can bolster a company's reputation among consumers, investors and other stakeholders. It demonstrates that the company is committed to making a positive impact beyond profit-making.

2) Improved Customer Loyalty

Customers are increasingly drawn to brands that are socially responsible. By aligning with causes that resonate with their target audience.

3) Operational Cost Savings

Investing in operational effeciencies results in operational cost savings as well as reduced environmental impact.

4) Retaining key and talented employees

Employees often stay longer and are more committed to their firm knowing that they are working for a business that practices CSR.

5) Easier access to funding

Many investors are more willing to support a business that practices CSR.

6) Reduced regulatory burden

Strong relationships with regulatory bodies can help to reduce a firm's regulatory burden.

* Corporate Social Responsibility and Good Business Ethics (Importance)

1) Gaining the goodwill of the company

- The goodwill that CSR activities generate can make it easier for corporations to conduct their business.

- for example, a company known for treating its employees well will find it easier to compete for the top job candidates.

- On the other hand, businesses that are not socially responsible run the risk of alienating their customer base.

2) Creating an Organization that operates consistently

- Organizations develop and abide by values to create an organizational culture and define a consistent approach for dealing with the needs of their stakeholders - shareholders, employees, customers, suppliers and the community.

- Consistency also means that shareholders customers, suppliers, and the community know what they can expect of the organization - that it will behave in the future much as it has in the past.

3) Fostering Good Business Practices

- Companies that produce safe and effective products avoid costly recalls and lawsuits.

- Companies that provide excellent service retain their customers instead of losing them to competitors.

- Companies that develop and maintain strong employee relations enjoy lower turnover rates and better employee morale.

- Suppliers and other business partners often place a priority on working with companies that operate in a fair and ethical manner.

4) Avoiding Unfavourable Publicity

- The public reputation of a company strongly influences the value of its stock, how consumers regard its products and services, the degree of oversight it receives from government agencies, and the amount of support and cooperation it receives from its business partners.

- If the organization is perceived as operating ethically, customers, business partners, shareholders, customer advocates, financial institutions, and regulatory bodies will usually regard it more favorably.

* Practices for Increasing business ethics.

1) Appoint a Corporate Ethics Officer
2) Require the Board of Directors to set and Model High Ethical Standards
3) Establish a Corporate code of ethics
4) Conduct Social Audits
5) Require Employees to take Ethics Training
6) Include Ethical Criteria in Employee Appraisals
7) Create an Ethical Work Environment

* Ethical Considerations in Decision Making

1) Develop Problem Statement

- Development of Problem statement is the most critical step in the decision-making proces

- If the problem is stated incorrectly, the chances of solving the real problem are greatly diminished.

2) Identify Alternatives

- In this stage of decision making, it is ideal to enlist the help of others, including stakeholders, to identify several alternatives to the problem.

- Brainstorming with others will increase your chances of identifying a broad range alternatives and determining the best solution.

3) Choose Alternative

- Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as effectiveness of addressing the issue, the extent of risk associated with each alternative cost, and time to implement.

- An alternative that sounds attractive but that is not feasible will not help the problem.

- As part of the evaluation process, weigh various laws, guidelines, and principles that may apply.

4) Implement the Decision

- Once an alternative is selected, it should be implemented in an effective, efficient, and timely manner.

- A transistion plan must be defined to explain to people how they will move from the old way of doing things to the new way.

- It may be necessary to train the people affected, provide incentives for making the change in a successful fashion, and modify the reward system to encourage new behaviours consistent to the change.

5) Evaluate the Results.

- After the solution to the problem has been implemented, monitor the results to see if the desired effect was achieved and observe its impact on the organization and the various stakeholders.

* Ethics in Information Technology

Key aspects of ethics in IT are :-

i) Privacy

Respecting individual's privacy rights by protecting their personal data and ensuring it's only used for intended purposes.

ii) Security

Safeguarding systems, networks, and data from unauthorised access, breaches and cyberattacks

iii) Transparency

Users should be informed about the types of data collected, the purposes for which it's used, and any third parties with whom it's shared.

iv) Accessibility

Ensuring that technology and digital content are accessible to all the individuals, including those with disabilities.

v) Fairness

This includes avoiding bias in algorithms and decision-making systems and considering the potential impact of technology on different groups within society.

vi) Environmental Impact

Considering the environmental impact of IT operations and technologies. This includes minimizing energy consumption, reducing electronic waste, and adopting sustainable practices in the design, manufacturing and disposal of IT equipment.

* Common Ethical Issues for IT Users

- Software Piracy
- Inappropriate use of Computer Resources
- Inappropriate sharing of Information

* Supporting the ethical Practices of IT Users

- Establishing guidelines for use of company hardware and software
- Defining an Acceptable Use Policy
- Structuring Information Systems to Protect Data and Information
- Installing and maintaining a corporate firewall
- Compliance