Security Policies:- A security policy is a "living document," meaning that the document is never finished and is continuously updated as technology and employee requirements change. The security policy translates, clarifies, and communicates the management position on security as defined in high-level security principles. The security policy acts as a bridge between these management objectives and specific security requirements. It informs users, staff, and managers of their obligatory requirements for protecting technology and information assets. The three reasons for having a security policy are as follows:

- To inform users, staff, and managers
- To specify mechanisms for security
- To provide a baseline

Why Policies should be developed:- A properly defined why security policy should be develop:

- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, probe, and investigate
- Define and authorize the consequences of violations
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation
- Ensure the confidentiality, integrity and availability of their data
- Provide a framework within which employees can work, are a reference for best practices, and are used to ensure users comply with legal requirements

WWW policies:- World Wide Web and Internet play an important role in providing access to information. Web means to support their mission and goal.WWW policy uses the following points :

- Offensive and harassing material should not made accessible via the company websites.
- The confidential matter should not be made available on the website of the organization.
- Personal material on the organizational website should not be given space .
- Personal /commercial advertising should not made available through company's website.
- Installation of web servers should be prohibited for the users of an organization.

Email Security policies:- This email policy accomplishes three objectives:

1. **Commercial objective**: in teaching employees how to send effective emails and stating target answering times, you can professionalize your email replies and therefore gain competitive advantage.
2. **Productivity objective**: by setting out rules for the personal use of email you can improve productivity and avoid misunderstandings.
3. **Legal objective**: in clearly stating what is considered as inappropriate email content you can minimize the risk of law suits and minimize employer's liability by showing that the company warned employees of inappropriate email use.

Creating an E-Mail Policy: Before you start creating an email policy, do some investigation into already existing company policies, such as guidelines on writing business letters, access to confidential information, personal use of the telephone systems and harassment at work. It is important that your email policy is compatible with your company's existing policies. You will also need to decide whether your company is going to allow personal use of the email system, and if so, to what extent. The email policy should be drafted with the help of human resources, IT and board of directors in order to reflect all viewpoints in the organization. It is also advisable to have several employees look at the policy and provide their feedback. Make sure that your policy is not so restrictive that it will compromise your employees' morale and productivity.

Sample E-Mail Policy:

Commercial: guidelines on how to write effective emails

- Corporate email style (formal/informal). This could include guidelines on salutation and ending of messages.
- What kind of signatures should be used, i.e. should signatures include company name, job function, telephone & fax number, address, website and/or a corporate slogan.
- Basic rules on how to write email messages.
- Expected time in which emails should be answered. For example, you could set a general rule that each email should be answered within at least 8 working hours, but 50% of emails should be answered within 4 hours.
- How to determine which emails should receive priority.
- When to send cc: or bcc: messages and what to do when you receive them.
- How and when to forward email messages and how you should handle forwarded messages.

Productivity Aspect : rules on the usage of the email system:

- Whether personal e-mails are accepted and if so, to what extent. For instance you could limit the amount of personal emails sent each day, or you could require personal emails to be saved in a separate folder. You could also limit or eliminate certain email attachments from being sent or received, and include rules on sending chain letters. Include examples and clear measures taken when these rules are breached.
- Use of newsletters & news groups. For instance you can require a user to request permission to subscribe to a newsletter or news group.
- Warn users that they should not engage in non-business activities that unnecessarily tie up network traffic.

Legal: prohibit inappropriate email content and warn of risks:

- Include a list of 'email risks' to make users aware of the potential harmful effects of their actions. Advise users that sending an email is like sending a postcard: if you don't want it posted on the bulletin board, then don't send it.
- The policy should expressly state that the email system is not to be used for the creation or distribution of any offensive, or disruptive messages, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability. State that employees who receive any emails with this content should report the matter to their supervisor immediately. Furthermore, mention that employees should not use email to discuss competitors, potential acquisitions or mergers or to give their opinion about another firm. Unlawful messages, such as copyright infringing emails should also be prohibited. Include examples and clear measures taken when these rules are breached.
- If you are going to monitor the content of your employees' emails, you must mention this in your email policy (In most countries/states you are allowed to monitor your employees' emails if your employees are made aware of this). Warn that employees should have no expectation of privacy in anything they create, store, send or receive on the company's computer system and that any of their messages may be viewed without prior notice.

Policy Review Process:- The process of review is divided into 6 steps:

1. Review to done by some who was not a part of the review writing team.
2. Policy to be assessed on the basis of completeness:

   (a) Policy framework to be accessed.
   (b) Policy elements to be accessed.

3. Policy statement should be reviewed on the following parameters:

   (a) Clarity
   (b) Conciseness
   (c) Exactness
   (d) Measurability
   (e) Practical
   (f) Feasibility
   (g) Timely

4. Review ensures that the policy answer the 5 W's

   (a) What is Information Security?
   (b) Why do you need Information Security?
   (c) Who is responsible for Information Security?
   (d) When is the right time to address Information Security?
   (e) Where does Information Security apply?

5. To check the consistency with the other policies, laws and regulations.
6. To check the availability of the updated policy to all members of the organization.

Corporate policies:- A Corporate policy aims on achieving its long term target by encapsulating its mission vision and objective and also for strategic decision- making.

- Vision and Mission
- Objectives
- Strategic decision-making

Sample Security Policies:-

1. Purpose

2. Aims and Commitments

3. Responsibilities

4. Risk Assessment and the Classification of Information

    - Risk assessment of information held
    - Personal Data

5. Protection of Information Systems and Assets

6 Protection of Confidential Information

    - Storage
    - Access
    - Remote access
    - Copying
    - Disposal
    - Use of portable devices or media
    - Exchange of Information and use of Email
    - Cryptographic controls
    - Backup
    - Further information
    - Hard Copies
    - Enforcement- Any loss or unauthorized disclosure must be promptly reported to the owner of the information.

7. Compliance

8. Appendix 1 Sample Risk Assessment

    1. Scope, Criteria and Organization

    2. Risk Identification and Analysis

        - Assets
        - Threats and Risks
        - Vulnerabilities

Publishing and Notification Requirement of the Policies:- Present our statements in an accurate, concise, readable and organized manner. Specifically, we must:

- Publish the report by the deadline.
- Include the required policy statements.
- Determine who gets the report.
- Distribute the report
- Retain record associated with the report.

Information Security Standards (ISO):- The ISO was established in 1947.It is collaborated with ITU(International Telecommunications Union) and IEC(International Electro technical Commission).

ISO/IEC 27001 - Information security management:

The ISO 27000 family of standards helps organizations keep information assets secure, using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

What is an ISMS?

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.

Certification to ISO/IEC 27001:

Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not obligatory. Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed. ISO does not perform certification.

Note: ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system". ISO 27001 uses a top down, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

1. Define the scope of the ISMS.
2. Conduct a risk assessment.
3. Manage identified risks.
4. Select control objectives and controls to be implemented.
5. Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organization. The 27001 standard does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the

accompanying code of practice, ISO/IEC 27002:2005. This second standard describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.ISO 27002 contains 12 main sections:

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

Organizations are required to apply these controls appropriately in line with their specific risks. Third-party accredited certification is recommended for ISO 27001 conformance. Other standards being developed in the 27000 family are:

- 27003 – Implementation guidance.
- 27004 - an information security management measurement standard suggesting metrics to help improve the effectiveness of an ISMS.
- 27005 – an information security risk management standard. (Published in 2008)
- 27006 - a guide to the certification or registration process for accredited ISMS certification or registration bodies. (Published in 2007)
- 27007 – ISMS auditing guideline.

IT Act:- An IT Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The **13** Chapters and **90** sections of the Act are listed below:

Chapter 1: Preliminary- this chapter covers section 1 to section 2.
Section 1: Short Title, Extent, Commencement and Application
Section 2: Definitions

Chapter 2: Digital Signature and Electronic Signature- this chapter covers section 3 to section 3A.

Section 3: Authentication of Electronic Records
Section 3A: Electronic Signature

Chapter 3: Electronic Governance- this chapter covers section 4 to section 10A.

Section 4: Legal Recognition of Electronic Records
Section 5: Legal recognition of Electronic Signature
Section 6: Use of Electronic Records and Electronic Signature in Government and its agencies
Section 6A: Delivery of Services by Service Provider
Section 7: Retention of Electronic Records
Section 7A: Audit of Documents etc in Electronic form
Section 8: Publication of rules, regulation, etc, in Electronic Gazette
Section 9: Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form
Section 10: Power to Make Rules by Central Government in respect of Electronic Signature
Section 10A: Validity of contracts formed through electronic means

Chapter 4: Attribution Acknowledgment and Dispatch of Electronic Records- this chapter covers section 11 to section 13.

Section 11: Attribution of Electronic Records
Section 12: Acknowledgement of Receipt
Section 13: Time and place of dispatch and receipt of electronic record

Chapter 5: Secure Electronic Records and Secure Electronic Signatures- this chapter covers section 14 to section 16.

Section 14: Secure Electronic Record
Section 15: Secure Electronic Signature
Section 16: Security procedures and Practices

Chapter 6: Regulation of Certifying Authorities- this chapter covers section 17 to section 34.

Section 17: Appointment of Controller and other officers
Section 18: The Controller may perform all or any of the following functions
Section 19: Recognition of foreign Certifying Authorities
Section 20: Omitted vide Information Technology Act, 2006
Section 21: License to issue electronic signature certificates
Section 22: Application for licence
Section 23: Renewal of licence
Section 24: Procedure for grant or rejection of licence
Section 25: Suspension of licence
Section 26: Notice of suspension or revocation of licence
Section 27: Power to delegate
Section 28: Power to investigate contraventions
Section 29: Access to computers and data
Section 30: Certifying Authority to follow certain procedures
Section 31: Certifying Authority to ensure compliance of the Act, etc
Section 32: Display of licence
Section 33: Surrender of licence
Section 34: Disclosure

Chapter 7: Electronic Signature Certificates- this chapter covers section 35 to section 39.
- Section 35: Certifying Authority to issue Electronic Signature Certificate
- Section 36: Representations upon issuance of Digital Signature Certificate
- Section 37: Suspension of Digital Signature Certificate
- Section 38: Revocation of Digital Signature Certificate
- Section 39: Notice of suspension or revocation

Chapter 8: Duties Of Subscribers- this chapter covers section 40 to section 42.
- Section 40: Generating Key Pair
- Section 40A: Duties of subscriber of Electronic Signature Certificate
- Section 41: Acceptance of Digital Signature Certificate
- Section 42: Control of Private key

Chapter 9: Penalties Compensation And Adjudication- this chapter covers section 43 to section 47.
- Section 43: Penalty and Compensation for damage to computer, computer system, etc
- Section 43A: Compensation for failure to protect Data
- Section 44: Penalty for failure to furnish information, return, etc
- Section 45: Residuary Penalty
- Section 46: Power to Adjudicate
- Section 47: Factors to be taken into account by the adjudicating officer

Chapter 10: The Cyber Appellate Tribunal- this chapter covers section 48 to section 64.
- Section 48: Establishment of Cyber Appellate Tribunal
- Section 49: Composition of Cyber Appellate Tribunal
- Section 50: Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal
- Section 51: Term of office, conditions of service etc of Chairperson and Members
- Section 52: Salary, allowance and other terms and conditions of service of Chairperson and Member
- Section 52A: Powers of superintendence, direction, etc
- Section 52B: Distribution of Business among Benches
- Section 52C: Powers of the Chairperson to transfer cases
- Section 52D: Decision by majority
- Section 53: Filling up of vacancies
- Section 54: Resignation and removal
- Section 55: Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings
- Section 56: Staff of the Cyber Appellate Tribunal
- Section 57: Appeal to Cyber Regulations Appellate Tribunal
- Section 58: Procedure and Powers of the Cyber Appellate Tribunal
- Section 59: Right to legal representation
- Section 60: Limitation
- Section 61: Civil court not to have jurisdiction
- Section 62: Appeal to High court
- Section 63: Compounding of Contravention
- Section 64: Recovery of Penalty or compensation

Chapter 11: Offences- this chapter covers section 65 to section 78.
- Section 65: Tampering with Computer Source
- Section 66: Computer Related Offences
- Section 66A: Punishment for sending offensive messages through communication service, etc.
- Section 66B: Punishment for dishonestly receiving stolen computer resource or

communication device
Section 66C: Punishment for identity theft
Section 66D: Punishment for cheating by personation by using computer resource
Section 66E: Punishment for violation of privacy
Section 66F: Punishment for cyber terrorism
Section 67: Punishment for publishing or transmitting obscene material in electronic form
Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
Section 67 C: Preservation and Retention of information by intermediaries
Section 68: Power of Controller to give directions
Section 69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
Section 69A: Power to issue directions for blocking for public access of any information through any computer resource
Section 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
Section 70: Protected system
Section 70 A: National nodal agency
Section 70 B: Indian Computer Emergency Response Team to serve as national agency for incident response
Section 71: Penalty for misrepresentation
Section 72: Breach of confidentiality and privacy
Section 72 A: Punishment for Disclosure of information in breach of lawful contract
Section 73: Penalty for publishing electronic Signature Certificate false in certain particulars
Section 74: Publication for fraudulent purpose
Section 75: Act to apply for offence or contraventions committed outside India
Section 76: Confiscation
Section 77: Compensation, penalties or confiscation not to interfere with other Punishment
Section 77A: Compounding of Offences
Section 77B: Offences with three years imprisonment to be cognizable
Section 78: Power to investigate offences

Chapter 12: Intermediaries Not To Be Liable In Certain Cases- this chapter covers section 79.
Section 79: Exemption from liability of intermediary in certain cases

Chapter 12A: Examiner Of Electronic Evidence- this chapter covers section 79A.
Section 79A: Central Government to notify Examiner of Electronic Evidence

Chapter 13: Miscellaneous- this chapter covers section 80 to section 90.
Section 80: Power of Police Officer and Other Officers to Enter, Search, etc
Section 81: Act to have Overriding effect
Section 81A: Application of the Act to Electronic cheque and Truncated cheque
Section 82: Chairperson, Members, Officers and Employees to be Public Servants
Section 83: Power to Give Direction
Section 84: Protection of Action taken in Good Faith
Section 84A: Modes or methods for encryption
Section 84B: Punishment for abetment of offences

Section 84C: Punishment for attempt to commit offences
Section 85: Offences by Companies
Section 86: Removal of Difficulties
Section 87: Power of Central Government to make rules
Section 88: Constitution of Advisory Committee
Section 89: Power of Controller to make Regulations
Section 90: Power of State Government to make rules

Chapter 1- This chapter contains the scope of the act.

Chapter II- of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -
rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.The said chapter also details the legal recognition of Digital Signatures.

Chapter IV- of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter V-The Security procedure and techniques to be used for the security of electronic records and digital signatures is taken care of in this chapter.

Chapter VI- covers regulation of certifying authorities.
Chapter VII - the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter VIII- Roles & responsibilities of subscribers.
Chapter IX- of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.
Chapter X- of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.
Chapter XI- of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

Intellectual Property Rights (IPR): Intellectual Property (IP) refers to the protection of creations of the mind, which have both a moral and a commercial value. IP law typically grants the author of an intellectual creation exclusive rights for exploiting and benefiting from their creation. However, these rights, also called monopoly right of exploitation, are limited in scope, duration and geographical extent. IP confers on individuals, enterprises or other entities the right to exclude others from the use of their creations. Consequently, intellectual property rights (IPRs) may have a direct and substantial impact on industry and trade as the owner of an IPR may through the enforcement of such a right - prevent the manufacture, use or sale of a product which incorporates the IPR.

Cyber Laws in India:- Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation(damage) all of which are subject to the Indian Penal Code(IPC). The unlawful of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. We can categorize Cyber crimes in two ways:
Computer as a Target : -using a computer to attack other computers. Example- Hacking, Virus/Worm attacks, DOS attack etc.

Computer as a weapon :- using a computer to commit real world crimes. Example Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber law in India :- When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India. Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace.

Copyright Act:

(1) For the purposes of this Act, "copyright" means the exclusive right, by virtue of and subject to the provisions of, this Act-

(a) In the case of a literary, dramatic or musical work, to do and authorize the doing of any of the following acts, namely:-

(i) to reproduce the work in any material form

(ii) to publish the work

(iii) to perform the work in public

(iv) to produce, reproduce, perform or publish any translation of the work

(vi) to communicate the work by radio-diffusion or to communicate to the public by a loud-speaker or any other similar instrument the radio-diffusion of the work

(vii) to make any adaptation of the work

(viii) to do in relation to a translation or an adaptation of the work any of the acts specified in relation to the work in clauses (i) to (vi)

(b) In the case of an artistic work, to do or authorize the doing of any of the following acts, namely-

(i) to reproduce the work in any material form

(ii) to publish the work

(iii) to include the work in any cinematograph film

(iv) to make any adaptation of the work

(v) to do in relation to an adaptation of the work any of the acts specified in relation to the work in clauses (i) to (iii).

(c) In the case of a cinematograph film, to do or authorize the doing of any of the following acts, namely:-

(i) to make a copy of the film

(ii) to cause the film, in so far as it consists of visual images, to be seen in public and, in so far as it consists of sounds, to be heard in public

(iii) to make any record embodying the recording in any part of the sound track associated with the film by utilizing such sound track

(iv) to communicate the film by radio-diffusion

(d) In the case of a record, to do or authorize the doing of any of the following acts by utilizing the record, namely:-

(i) to make any other record embodying the same recording

(ii) to cause the recording embodied in the record to be heard in public

(iii) to communicate the recording embodied in the record by radio-diffusion.

Intellectual Property Law:- Intellectual property law deals with the rules for securing and enforcing legal rights to inventions, designs, and artistic works. Just as the law protects ownership of personal property and real estate, so too does it protect the exclusive control of intangible assets.

The purpose of these laws is to give an incentive for people to develop creative works that benefit society, by ensuring they can profit from their works without fear of misappropriation by others. The WTO (World Trade Organization) agreement consists of an agreement on Trade-

Related Aspects of Intellectual Property Rights(TRIPS). The creator/inventor gets exclusive rights against any misuse or use of work without his/her prior information. However, the rights are granted for a limited period of time to maintain equilibrium. TRIPS prescribes the seven areas of Intellectual Property.

- **Copyrights**: Copyright. Original creative works such as paintings, writing, architecture, movies, software, photos, dance, and music are protected by federal copyright law. A work must meet certain minimum requirements to qualify for copyright protection Trademarks
- **Trademark**: Brand names such as Nike and Avis, as well as logos, slogans, and other devices that identify and distinguish products and services, are protected under federal and state trademark laws. Unlike copyrighted works, trademarks receive different degrees of protection depending on numerous variables, including the consumer awareness of the trademark, the type of service and product it identifies, and the geographic area in which the trademark is used.
- **Geographical Indication:** A geographical indication (GI) is a sign that identifies a product as originating from a particular location which gives that product a special quality or reputation or other characteristic. Well-known examples of GIs include Bordeaux (wine), Darjeeling (tea) and Tuscany (olive oil).
- **Industrial Design** : An Industrial Design is the ornamental aspect of a useful article. This ornamental aspect may be constituted by elements, which are three-dimensional (the shape of the article) or two-dimensional (lines, designs, patterns and colours) but must not be dictated solely or essentially by technical or functional considerations. It is the right to protect the ornamental, non-functional features of an Industrial Article or Product that arise from Design Activity. To be eligible for Industrial Design Protection in this country, Industrial Designs must be Original or Novel and must be Registered at the Intellectual Property Office. Example: The shapes of many ergonomically designed pieces of furniture, tools, tool handles, boat hulls and sunglasses are just a smattering of the many shapes around us that are protected by Industrial Design

- **Patents:** Patents are granted by national or regional patent offices. A given patent is therefore only useful for protecting an invention in the country in which that patent is granted.

- **Layout Designs:** the design or arrangement of something <the layout of the park>
- **Protection of undisclosed information**: In the course of ensuring effective protection against unfair competition as provided in Article . Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question.

(b) has commercial value because it is secret.

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Advantages of Intellectual Property Rights:

Intellectual property rights are advantageous in the following ways –

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.

Software License: A software license is a legally binding agreement that specifies the terms of use for an application and defines the rights of the software producer and of the end-user. All software must be legally licensed before it may be installed. Proof of purchase (purchase orders, receipts, invoices or similar documentation are acceptable) must be maintained by individuals or departments for all non-ITS provided software that is installed on a university owned computer.

Types of Software License:

1) **Paid License:**-Time-based, User based, Feature based

2) **Freeware License:** no fee is to be paid**.**

Semiconductor Law:

1. **Semiconductor Integrated Circuit:** Semiconductor Integrated Circuit means a product having transistors and other circuitry elements, which are inseparably formed on a semiconductor material or an insulating material or inside the semiconductor material and designed to perform an electronic circuitry function.

2. **Layout-design**: The layout-design of a semiconductor integrated circuit means a layout of transistors and other circuitry elements and includes lead wires connecting such elements and expressed in any manner in semiconductor integrated circuits. Criteria for Registration of a Chip Layout Design

    - Original
    - Distinctive
    - Capable of distinguishing from any other lay-out design.