**CYBER SECURITY**

**(UNIT 4)**

**SUBJECT CODE:AUC-002**

**SEMESTER: 4**

**SESSION: 2016-2017**

**Security Policies**

Security policy is a definition of what it means to *be secure* for a [system](https://en.wikipedia.org/wiki/System), organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

**Significance**

If it is important to be secure, then it is important to be sure all of the security policy is enforced by mechanisms that are strong enough. There are many organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as [information systems](https://en.wikipedia.org/wiki/Information_systems), policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. However, this practice has pitfalls. It is too easy to simply go directly to the sub-policies, which are essentially the rules of operation and dispense with the top level policy. That gives the false sense that the rules of operation address some overall definition of security when they do not. Because it is so difficult to think clearly with completeness about security, rules of operation stated as "sub-policies" with no "super-policy" usually turn out to be rambling rules that fail to enforce anything with completeness. Consequently, a top-level security policy is essential to any serious security scheme and sub-policies and rules of operation are meaningless without it.

|  |
| --- |
| **Why Do You Need a Security Policy?**Who is responsible for securing an organization's **information**?  Perhaps the Research and Evaluation department?  Not exactly.  The Management Information System (MIS) staff?  Wrong again.  Ultimately, it is not only individual employees or departments that are responsible for the security of **confidential information**, but also the institution itself. It is, therefore, incumbent upon top administrators, who are charged with protecting the institution's best interests, to ensure that an appropriate and effective **security policy** is developed and put into practice throughout the organization. https://nces.ed.gov/pubs98/safetech/Images/blank.GIF |
| While policies themselves don't solve problems, and in fact can actually complicate things unless they are clearly written and observed, policy does define the ideal toward which all organizational efforts should point.  By definition, security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it.  Good policy protects not only information and systems, but also individual employees and the organization as a whole.  It also serves as a prominent statement to the outside world about the organization's commitment to security. https://nces.ed.gov/pubs98/safetech/Images/blank.gif |
|   |   |  |

**WWW Policy :** The Internet is a network of networks providing various services such as sending e-mails, transferring files, login from remote systems, and WWW. The WWW is the universe of the Internet-accessible information. While browsing the Internet, there are various risks. Some of which are as follows:

* The software provided to the employess for business use can be used for any for profit outside business activity or potentially embaress the company.
* The software or documents downloaded over the WWW can contain virus.
* The users of an organization while browsing the Internet can access sites containing offensive materials.

To avoid such risks, the organization needs to define the WWW policy. Some examples of WWW policy are as follows:

* No Offensive or harassing material may be made available through company websites.
* No personal commercial advertising should be made available through company websites.
* No company confidential material should be made available.
* Users of an organization should not be permitted to insall or run Web servers.
* The personal material on or accessible from the website should be minimal.

**E-mail Security Policies**

E-mails can be used not only to improve the communication between employees, but also to transmit proprietary information, harass other users,engage in illegal activities, and serve as evidence against the company in legal actions. E-mail is actually the electronic version of a postcard and requires special policy considerations from archiving to content guidelines. Therefore, the organizations should take various points into consideration while writing e-mail policies.There are different aspects to email security policies, it can be broken into four main parts.

1. **Automatically Forwarded Email Policy**. The idea here is that no automatic forwarding of email will be set up without management approval and to lay out the rules for employees about the consequences of forwarding sensitive information out of the company.
2. **General Email Policy.** This is an email policy designed to protect the companies reputation. Also referred to as email usage policy. This policy will cover what is acceptable use of email in the work place. It will specify what is unacceptable such as email being used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin
3. **Email Retention Policy**. The Email retention policy clearly explains to employees what information needs to be kept and for how long. Although there should be a policy on this the management of the data should be automated by the organisation if possible depending on its size. Obviously if each employee had to take responsibility for the minutiae of email retention without the assistance of an email archiving service it would seriously hinder productivity
4. **Email Security Policy**. Here is where our advice differs from others. If not included in the other policies some security rules need to be put in place regarding how to report Phishing emails to the security team and other risky looking emails. The employee expectations should be listed. It is also important that a procedure is put in place for them to report the emails and forward them as an attachment to the security team.

**Policy Review Process**

1. The basic methodology for process reviews will involve a review by a panel of one organization process manager not of the process being reviewed, and one organization client of the process being reviewed, augmented by at least two external experts.
2. A reference group consisting of relevant organisation process managers and process clients will be established to develop the necessary review documentation.
3. The review process will include some or all of the following elements:
	* circulation of a discussion paper addressing details of the process and an analysis of its current level of effectiveness,
	* a survey of stakeholders and users,
	* submissions from stakeholders and users,
	* a survey of the application of the process at similar institutions, and
	* determination of best practice for the process within and without the sector.



1. The review process will be conducted in the spirit of modern quality management approaches:
	* involving a no blame environment,
	* reviewing the process as a whole rather than individuals,
	* being supportive of staff involved in managing the process,
	* performed in the interest of continuous improvement,
	* identifying solutions, and
	* geared towards a celebration of achievements.

	The review process must also be information-driven, basing its decisions and conclusions on sound data and well-developed information.
2. The review process must involve:
	* a clear characterisation of the process elements,
	* a clear articulation of the aims of the process,
	* a review of associated policies and practices,
	* an objective assessment of the success of the process in meeting these aims involving wide consultation with all stakeholder groups and analysis involving qualitative and quantitative data, and
	* recommendations as to how the process might be improved, with an action plan for implementing these recommendations.
3. The review process must be forward-looking and strategic, using an analysis of past performance as a basis for refining the setting of objectives, reviewing strategies and ensuring continuous improvement, plus enhancing efficiencies.
4. The action plan will be written to ensure that the responsibility for implementing individual recommendations are clearly identified so as to facilitate a review of performance of the action plan, which will be required to be submitted to the Planning, Quality and Review Committee two years after the initial review. This process will be coordinated by the Pro-Vice-Chancellor (Planning and Quality).
5. The review process must not impose an undue burden on members of staff and not impede the normal operations of the organisational sections concerned. In particular, the review should draw on existing documentation and available data as much as possible.

**Corporate Policies**

A formal [declaration](http://www.investorwords.com/13155/declaration.html) of the [guiding principles](http://www.investorwords.com/16036/guiding_principles.html) and procedures by which a company will operate typically established by its [board of directors](http://www.investorwords.com/511/Board_of_Directors.html) or a [senior](http://www.investorwords.com/4485/senior.html) [management](http://www.investorwords.com/2931/management.html) [policy](http://www.investorwords.com/3728/policy.html) committee. Imbedded in corporate policy are the [company's](http://www.investorwords.com/992/company.html) mission [statement](http://www.investorwords.com/4701/statement.html), [objectives](http://www.investorwords.com/3372/objective.html) and the [principles](http://www.investorwords.com/3845/principle.html) by which strategic [decisions](http://www.investorwords.com/19281/decision.html) are to be made. It also [forms](http://www.investorwords.com/13345/form.html) the basis for measuring [performance](http://www.investorwords.com/3665/performance.html) and ensuring [accountability](http://www.investorwords.com/15730/accountability.html) at all [levels](http://www.investorwords.com/10180/level.html) of the company

Usually, a documented set of broad guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. Formulated by the firm's board of directors, corporate policy lays down the firm's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy, and directs and restricts the plans, decisions, and actions of the firm's officers in achievement of its objectives. Also called company policy.

**Sample Security Policies**

A security policy is the essential basis on which an effective and comprehensive security program can be developed. This critical component is the primary way in which the agency security plan is translated into specific, measurable, and testable goals and objectives.

The security policies developed must establish a consistent notion of what is and what is not permitted with respect to control of access to your information resources. They must bond with the business, technical, legal, and regulatory environment of your agency.

The following is a recommended outline of the components and characteristics of a security policy template .

Section 1 – Introduction:

A purpose should be stated in the introduction section. This should provide the reader with a brief description of what this policy will state and why it is needed. The security stance of your agency should be stated here.

Section 2 – Roles and Responsibilities:

It is important that the policy detail the specific responsibilities of each identifiable user population, including management, employees and residual parties.

Section 3 – Policy Directives:

This section describes the specifics of the security policy. It should provide sufficient information to guide the development and implementation of guidelines and specific security procedures.

Section 4 – Enforcement, Auditing, Reporting:

This section states what is considered a violation and the penalties for non-compliance. The violation of a policy usually implies an adverse action which needs to be enforced.

Section 5 – References:

This section lists all references mentioned in the policy, including agency standards, procedures, government code, and State Administrative Manual sections.

Section 6 – Control and Maintenance:

This section states the author and owner of the policy. It also describes the conditions and process in which the policy will be reviewed. A policy review should be performed at least on an annual basis to ensure that the policy is current.

**Information Security Standards (ISO)**

The term "standard" is sometimes used within the context of [information security policies](https://en.wikipedia.org/wiki/Information_security_policies) to distinguish between written policies, standards and procedures. Organizations should maintain all three levels of documentation to help secure their environment. Information security policies are high-level statements or rules about protecting people or systems. (For example, a policy would state that "Company X will maintain secure passwords") A "standard" is a low-level prescription for the various ways the company will enforce the given policy. (For example, "Passwords will be at least 8 characters, and require at least one number.") A "procedure" can describe a step-by-step method to implementing various standards. (For example, "Company X will enable password length controls on all production Windows systems.")

This use of the term "standard" differs from use of the term as it relates to [information security](https://en.wikipedia.org/wiki/Information_security) and privacy frameworks, such as [ISO/IEC 27002](https://en.wikipedia.org/wiki/ISO/IEC_27002) or COBIT.

To effectively assess the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements. This process is difficult enough in a centralized data processing environment; with the use of local- and wide-area networks (LANs and WANs, respectively), the problems are compounded.

The challenges for management in providing information security are formidable. Even for relatively small organizations, information system assets are substantial, including databases and files related to personnel, company operation, financial matters, and so on. Typically, the information system environment is complex, including a variety of storage systems, servers, workstations, local networks, and Internet and other remote network connections. Managers face a range of threats always growing in sophistication and scope. And the range of consequences for security failures, both to the company and to individual managers, is substantial, including financial loss, civil liability, and even criminal liability.

Standards for providing information system security become essential in such circumstances. Standards can define the scope of security functions and features needed, policies for managing information and human assets, criteria for evaluating the effectiveness of security measures, techniques for ongoing assessment of security and for the ongoing monitoring of security breaches, and procedures for dealing with security failures.

**IT Act**

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the [Indian Parliament](https://en.wikipedia.org/wiki/Indian_Parliament)(No 21 of 2000) notified on 17 October 2000. It is the primary law in [India](https://en.wikipedia.org/wiki/India) dealing with [cybercrime](https://en.wikipedia.org/wiki/Cybercrime) and [electronic commerce](https://en.wikipedia.org/wiki/Electronic_commerce). It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997

The original Act contained 94 sections, divided in 13 chapters and 4 [schedules](https://en.wikipedia.org/wiki/Schedule). The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.[[3]](https://en.wikipedia.org/wiki/Information_Technology_Act%2C_2000#cite_note-PawarKolekar2015-3)

The Act provides legal framework for electronic governance by giving recognition to [electronic records](https://en.wikipedia.org/wiki/Electronic_records) and [digital signatures](https://en.wikipedia.org/wiki/Digital_signature). The formations of Controller of Certifying Authorities was directed by the Act, to regulation issuing of digital signatures. It also defined cyber crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law.[[3]](https://en.wikipedia.org/wiki/Information_Technology_Act%2C_2000#cite_note-PawarKolekar2015-3) The Act also amended various sections of [Indian Penal Code, 1860](https://en.wikipedia.org/wiki/Indian_Penal_Code), [Indian Evidence Act, 1872](https://en.wikipedia.org/wiki/Indian_Evidence_Act), Banker's Book Evidence Act, 1891, and [Reserve Bank of India Act, 1934](https://en.wikipedia.org/wiki/Reserve_Bank_of_India_Act%2C_1934) to make them compliant with new technologies.

### Amendments

A major amendment was made in 2008. It introduced the Section 66A which penalised sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for[child porn](https://en.wikipedia.org/wiki/Child_porn), [cyber terrorism](https://en.wikipedia.org/wiki/Cyber_terrorism) and [voyeurism](https://en.wikipedia.org/wiki/Voyeurism). It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

**Copyright Act**

Copyright is a bundle of rights given by the law to the creators of literary, dramatic, musical and artistic works and the producers of cinematograph films and sound recordings. The rights provided under Copyright law include the rights of reproduction of the work, communication of the work to the public, adaptation of the work and translation of the work. The scope and duration of protection provided under copyright law varies with the nature of the protected work.

The **Copyright Act, 1957** (as amended by the Copyright Amendment Act 2012) governs the subject of copyright law in [India](https://en.wikipedia.org/wiki/India). The history of copyright law in India can be traced back to its colonial era under the [British Empire](https://en.wikipedia.org/wiki/British_Empire). The [Copyright Act 1957](https://en.wikipedia.org/wiki/Copyright_Act%2C_1957) was the first post-independence copyright legislation in India and the law has been amended six times since 1957. The most recent amendment was in the year 2012, through the Copyright (Amendment) Act 2012.

India is a member of most of the important international conventions governing the area of copyright law, including the [Berne Convention of 1886](https://en.wikipedia.org/wiki/Berne_Convention_for_the_Protection_of_Literary_and_Artistic_Works) (as modified at Paris in 1971), the [Universal Copyright Convention of 1951](https://en.wikipedia.org/wiki/Universal_Copyright_Convention), the [Rome Convention of 1961](https://en.wikipedia.org/wiki/Rome_Convention_for_the_Protection_of_Performers%2C_Producers_of_Phonograms_and_Broadcasting_Organisations) and [the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)](https://en.wikipedia.org/wiki/Agreement_on_Trade-Related_Aspects_of_Intellectual_Property_Rights).[[5]](https://en.wikipedia.org/wiki/Copyright_law_of_India#cite_note-5) But India is not a member of the [WIPO Copyright Treaty](https://en.wikipedia.org/wiki/World_Intellectual_Property_Organization_Copyright_Treaty) (WCT) and the [WIPO Performances and Phonograms Treaty](https://en.wikipedia.org/wiki/WIPO_Performances_and_Phonograms_Treaty) (WPPT).

**Patent Law**

The word *patent* originates from the [Latin](https://en.wikipedia.org/wiki/Latin) *patere*, which means "to lay open" (i.e., to make available for public inspection). More directly, it is a shortened version of the term [*letters patent*](https://en.wikipedia.org/wiki/Letters_patent), which was a [royal decree](https://en.wikipedia.org/wiki/Royal_decree) granting exclusive rights to a person, predating the modern patent system.

A **patent** ([/ˈpætənt/](https://en.wikipedia.org/wiki/Help%3AIPA_for_English) or [/ˈpeɪtənt/](https://en.wikipedia.org/wiki/Help%3AIPA_for_English)) is a set of [exclusive rights](https://en.wikipedia.org/wiki/Exclusive_right) granted by a [sovereign state](https://en.wikipedia.org/wiki/Sovereign_state) to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an [invention](https://en.wikipedia.org/wiki/Invention). An invention is a solution to a specific technological problem and is a product or a process.Patents are a form of  [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property).

The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements. Typically, however, a granted patent application must include one or more [claims](https://en.wikipedia.org/wiki/Claim_%28patent%29) that define the invention. A patent may include many claims, each of which defines a specific property right. These claims must meet relevant [patentability](https://en.wikipedia.org/wiki/Patentability) requirements, such as [novelty](https://en.wikipedia.org/wiki/Novelty_%28patent%29), [usefulness](https://en.wikipedia.org/wiki/Usefulness), and [non-obviousness](https://en.wikipedia.org/wiki/Inventive_step_and_non-obviousness). The exclusive right granted to a patentee in most countries is the right to prevent others, or at least to try to prevent others, from commercially making, using, selling, importing, or distributing a patented invention without permission.

Under the [World Trade Organization](https://en.wikipedia.org/wiki/World_Trade_Organization)'s (WTO) [Agreement on Trade-Related Aspects of Intellectual Property Rights](https://en.wikipedia.org/wiki/Agreement_on_Trade-Related_Aspects_of_Intellectual_Property_Rights), patents should be available in WTO member states for any invention, in all fields of technology, and the [term of protection](https://en.wikipedia.org/wiki/Term_of_patent) available should be a minimum of twenty years. Nevertheless, there are variations on what is[patentable subject matter](https://en.wikipedia.org/wiki/Patentable_subject_matter) from country to country.

**Intellectual Property Rights (IPR)**

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by, for example, [patents](http://www.wipo.int/patents/en/), [copyright](http://www.wipo.int/copyright/en/) and [trademarks](http://www.wipo.int/trademarks/en/), which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

The term "Intellectual Property Rights" refers to the legal rights granted with the aim to protect the creations of the intellect. These rights include Industrial Property Rights (e.g. patents, industrial designs and trademarks) and Copyright (right of the author or creator) and Related Rights (rights of the performers, producers and broadcasting organisations).

Intellectual property rights include [patents](https://en.wikipedia.org/wiki/Patent), [copyright](https://en.wikipedia.org/wiki/Copyright), [industrial design rights](https://en.wikipedia.org/wiki/Industrial_design_right), [trademarks](https://en.wikipedia.org/wiki/Trademark), [plant variety rights](https://en.wikipedia.org/wiki/Plant_variety_rights), [trade dress](https://en.wikipedia.org/wiki/Trade_dress), and in some jurisdictions [trade secrets](https://en.wikipedia.org/wiki/Trade_secret). There are also more specialized or derived varieties of [*sui generis*](https://en.wikipedia.org/wiki/Sui_generis) exclusive rights, such as circuit design rights (called [mask work](https://en.wikipedia.org/wiki/Mask_work) rights in the US) and[supplementary protection certificates](https://en.wikipedia.org/wiki/Supplementary_protection_certificate) for pharmaceutical products (after expiry of a patent protecting them) and [database rights](https://en.wikipedia.org/wiki/Database_rights) (in [European law](https://en.wikipedia.org/wiki/EC_law)).

**Objectives Of Intellectual Property Rights**

The stated objective of most intellectual property law (with the exception of trademarks) is to "Promote progress."  By exchanging limited exclusive rights for disclosure of inventions and creative works, society and the patentee/copyright owner mutually benefit, and an incentive is created for inventors and authors to create and disclose their work. Some commentators have noted that the objective of intellectual property legislators and those who support its implementation appears to be "absolute protection". "If some intellectual property is desirable because it encourages innovation, they reason, more is better. The thinking is that creators will not have sufficient incentive to invent unless they are legally entitled to capture the full social value of their inventions". This absolute protection or full value view treats intellectual property as another type of "real" property, typically adopting its law and rhetoric. Other recent developments in intellectual property law, such as the [America Invents Act](https://en.wikipedia.org/wiki/America_Invents_Act), stress international harmonization. Recently there has also been much debate over the desirability of using intellectual property rights to protect cultural heritage, including intangible ones, as well as over risks of commodification derived from this possibility. The issue still remains open in legal scholarship.

**Cyber Laws In India**

Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of  law and regulation.

Since Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse 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

The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.

Legal aspects are an indispensable part of a successful business environment in any country. They reflect the policy framework and the mind set of the Governmental structure of that country. They ensure that every company is functioning as per the statutory framework of the country.

**Advantages of Cyber Laws**

* The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
* In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.
* From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
* Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
* Digital signatures have been given legal validity and sanction in the Act.
* The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
* The Act now allows Government to issue notification on the web thus heralding e-governance.
* The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
* The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

**Information Technology (IT) Act 2000 Provisions**

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. 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. Some highlights of the Act are listed below:

**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-VII** of 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-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 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.

Patents give inventors the right to use their product in the marketplace, or to profit by transferring that right to someone else. Depending on the type of invention, patent rights are valid for up to 20 years. Qualifying items include new machines, technological improvements, and manufactured goods, including the “look” of a product. Patent protection will be denied if an invention is found to be obvious in design, not useful, or morally offensive.

Trademarks protect symbols, names, and slogans used to identify goods and services. The purpose is to avoid confusion, deter misleading advertising, and help consumers distinguish one brand from another. Since the goal is to distinguish, generic or purely descriptive marks may not qualify. Rights can potentially last forever, and they are obtained by simply using a mark. While not required, owners can register their marks for additional protection.

Copyrights apply to writings, music, motion pictures, architecture, and other original intellectual and artistic expressions. Protection is not available for theories or ideas, or anything that has not been captured in a fixed medium. The act of creation itself produces a copyright and unpublished works are still protected. Use of a copyright symbol and date is common, but not mandatory. Most copyrights are valid for the creator’s lifetime, plus 70 years.

**Copyright Law**

The **Copyright Act, 1957** (as amended by the Copyright Amendment Act 2012) governs the subject of copyright law in [India](https://en.wikipedia.org/wiki/India). The history of copyright law in India can be traced back to its colonial era under the [British Empire](https://en.wikipedia.org/wiki/British_Empire). The [Copyright Act 1957](https://en.wikipedia.org/wiki/Copyright_Act%2C_1957) was the first post-independence copyright legislation in India and the law has been amended six times since 1957. The most recent amendment was in the year 2012, through the Copyright (Amendment) Act 2012.

India is a member of most of the important international conventions governing the area of copyright law, including the [Berne Convention of 1886](https://en.wikipedia.org/wiki/Berne_Convention_for_the_Protection_of_Literary_and_Artistic_Works) (as modified at Paris in 1971), the [Universal Copyright Convention of 1951](https://en.wikipedia.org/wiki/Universal_Copyright_Convention), the [Rome Convention of 1961](https://en.wikipedia.org/wiki/Rome_Convention_for_the_Protection_of_Performers%2C_Producers_of_Phonograms_and_Broadcasting_Organisations) and [the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)](https://en.wikipedia.org/wiki/Agreement_on_Trade-Related_Aspects_of_Intellectual_Property_Rights).[[5]](https://en.wikipedia.org/wiki/Copyright_law_of_India#cite_note-5) But India is not a member of the [WIPO Copyright Treaty](https://en.wikipedia.org/wiki/World_Intellectual_Property_Organization_Copyright_Treaty) (WCT) and the [WIPO Performances and Phonograms Treaty](https://en.wikipedia.org/wiki/WIPO_Performances_and_Phonograms_Treaty) (WPPT).

Copyright is a bundle of rights given by the law to the creators of literary, dramatic, musical and artistic works and the producers of cinematograph films and sound recordings. The rights provided under Copyright law include the rights of reproduction of the work, communication of the work to the public, adaptation of the work and translation of the work. The scope and duration of protection provided under copyright law varies with the nature of the protected work.

The Indian copyright law protects literary works, dramatic works, musical works, artistic works, cinematograph films and sound recordings.

**Software License**

A [software](http://searchsoa.techtarget.com/definition/software) license is a document that provides legally binding guidelines for the use and distribution of [software](http://searchsoa.techtarget.com/definition/software). Software licenses typically provide end users with the right to one or more copies of the software without violating [copyrights](http://searchsecurity.techtarget.com/definition/copyright). The license also defines the responsibilities of the parties entering into the license agreement and may impose restrictions on how the software can be used. Software licensing terms and conditions usually include [fair use](http://whatis.techtarget.com/definition/fair-use) of the software, the limitations of liability, warranties and disclaimers and protections if the software or its use infringes on the [intellectual property](http://whatis.techtarget.com/definition/intellectual-property-IP) rights of others.

A software license is a legal instrument (usually by way of [contract law](https://en.wikipedia.org/wiki/Contract_law), with or without printed material) governing the use or redistribution of software. Under United States copyright law: all [software](https://en.wikipedia.org/wiki/Software) is [copyright](https://en.wikipedia.org/wiki/Copyright) protected, in [source code](https://en.wikipedia.org/wiki/Source_code) as also [object code](https://en.wikipedia.org/wiki/Object_code) form. The only exception is [software in the public domain](https://en.wikipedia.org/wiki/Public_domain_software). A typical software license grants the [license](https://en.wikipedia.org/wiki/Licensee), typically an [end-user](https://en.wikipedia.org/wiki/End-user), permission to use one or more copies of software in ways where such a use would otherwise potentially constitute copyright infringement of the software owner's [exclusive rights](https://en.wikipedia.org/wiki/Exclusive_rights) under copyright law.

**Semiconductor Law**

 With the advancement of information technology, a new branch in the field of intellectual property flourished, called as the Layout-Design or the of the semiconductor integrated circuits.

The semiconductor integrated circuit is an integral part of every computer chip. The fifth generation computers are using Very Large Scale Integration (VLSI) where numerous transistors are accommodated on a single chip, cutting down the size of the chip and at the same time increasing it’s processing power significantly. This ultimately translates into smaller and more powerful computers. Hence, the development of the layout-design on a semiconductor integrated circuit as an intellectual property is quite significant.

Hence, a step was taken by various organizations to pass regulations regarding this issue. One such was the World Trade Organization, and the result was the TRIPS agreement addressing the intellectual property related issues. India being a signatory of the WTO also passed an Act in conformity with the TRIPS agreement called the Semiconductor Integrated Circuits Layout-Design Act (SICLDA) passed in the year 2000.

*"Semiconductor Integrated circuits Layout- Design Act 2000"* is a supplement act to designs. It fulfills the obligations of TRIPS agreement (Art.35 to 38) regarding the protection of semiconductor integrated circuits layout- designs.

Definitions

SICLD Act defines the following as:

* "Semiconductor integrated circuit" means a product having transistors or 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.
* "Layout-design" means a layout of transistors, and other circuitry elements and includes lead wires connecting such elements and expressed in any manner in a semiconductor integrated circuit.
* "Commercial exploitation" in relation to the SICLD means to sell, lease, offer or exhibit for sale or otherwise distribute such semiconductor integrated circuit for any commercial purpose.

**Need for Protection of IC designs**:

Product life cycles in many industries are shortening. The length of time and amount of investment required, to obtain intellectual property rights, especially patents, can be disproportionate to the life of such product. Requirements such as the need to mark products with "patent pending" also become impracticable when products have short life cycles and use many different technologies subject to different patents, especially when these products are miniaturized.

**Protection under Patent or other IP Laws:**

Integrated circuits comprises of numerous building blocks, each block being patentable. Since an integrated circuit contains hundreds or thousands of semiconductor devices, a claim to an integrated circuit would have to cover hundreds or thousands of individual elements. Consequently, a patent claim that attempts to describe an entire integrated circuit may be hundreds of pages long. Clearly, such a narrow claim would provide almost no protection. Even if one sought such narrow protection, writing a patent application supporting a claim with thousands of elements would be extremely complex, cumbersome, and expensive. Obviously, integrated circuits are not easily describable in a patent specification or the claims. Also, it may take several years to obtain an integrated circuit patent from most patent offices worldwide. This is unacceptable given that an integrated circuit’s useful commercial life may be less than one year. The cumbersome, time-consuming nature of filing combined with extremely narrow protection often makes patent law an insufficient form of protection for integrated circuits.

**Patent Law**

A patent is a set of [exclusive rights](https://en.wikipedia.org/wiki/Exclusive_right) granted by a [sovereign state](https://en.wikipedia.org/wiki/Sovereign_state) to an inventor or assigned for a limited period of time in exchange for detailed public disclosure of an [invention](https://en.wikipedia.org/wiki/Invention). An invention is a solution to a specific technological problem and is a product or a process. Patents are a form of [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property).

The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements. Typically, however, a granted patent application must include one or more [claims](https://en.wikipedia.org/wiki/Claim_%28patent%29) that define the invention. A patent may include many claims, each of which defines a specific property right. These claims must meet relevant [patentability](https://en.wikipedia.org/wiki/Patentability) requirements, such as [novelty](https://en.wikipedia.org/wiki/Novelty_%28patent%29), [usefulness](https://en.wikipedia.org/wiki/Usefulness), and [non-obviousness](https://en.wikipedia.org/wiki/Inventive_step_and_non-obviousness). The exclusive right granted to a patentee in most countries is the right to prevent others, or at least to try to prevent others, from commercially making, using, selling, importing, or distributing a patented invention without permission.

Under the [World Trade Organization](https://en.wikipedia.org/wiki/World_Trade_Organization)'s (WTO) [Agreement on Trade-Related Aspects of Intellectual Property Rights](https://en.wikipedia.org/wiki/Agreement_on_Trade-Related_Aspects_of_Intellectual_Property_Rights), patents should be available in WTO member states for any invention, in all fields of technology, and the [term of protection](https://en.wikipedia.org/wiki/Term_of_patent) available should be a minimum of twenty years. Nevertheless, there are variations on what is [patentable subject matter](https://en.wikipedia.org/wiki/Patentable_subject_matter) from country to country.

The Patent Act of 1790 was the first patent statute passed by the federal government of the [United States](https://en.wikipedia.org/wiki/United_States). It was enacted on April 10, 1790, about one year after the constitution was ratified and a new government was organized. The law was concise, defining the subject matter of a U.S. patent as “any useful art, manufacture, engine, machine, or device, or any improvement thereon not before known or used. It granted the applicant the "sole and exclusive right and liberty of making, constructing, using and vending to others to be used" of his invention.

**Procedure For Patent Registeration**

#### Step 1:  Write down the invention (idea or concept) with as much details as possible

Collect all the information about your invention such as:

* Area of invention
* Description of the invention what it does
* How does it work
* Advantages of the invention

#### Step 2:  include drawings, diagrams or sketches explaining working of invention

The drawings and diagrams should be designed so as to explain the working of the invention in better way with visual illustrations. They play an important role in patent application.

#### Step 3: check whether the invention is patentable subject matter

All inventions may not be patentable, as per Indian patent act there are certain inventions that are not patentable explained in detail in **(inventions not patentable)**

#### Step 4: Patentability search

The next step would be finding out whether your invention meets all patentability criteria as per Indian patent act such as:

* Novelty
* Non-obviousness
* Industrial application
* Enabling

#### Step 5: Decide whether to go ahead with patent

The patentability report and opinion helps you decide whether to go ahead with the patent or not, chances are what you thought as novel might already been patented or know to public in some form of information. Hence this reports saves lots of time, efforts and cost of the inventor by helping him decide whether to go ahead with the patent filing process or not.

**Step 6: Draft (write) patent application**

In case you are at very early stage in the research and development for your invention, then you can go for provisional specification. It gives following benefits:

* Secures filing date
* 12 months of time to file complete specification
* Low cost

#### Step 7: Publication of the application

Up on filing the complete specification along with application for patent, the application is published after 18 months of first filing. An early publication request can be made along with prescribed fees if you do not wish to wait till the expiry of 18 months from the date of filing for publishing your patent application.

Generally the patent application is published within a month form request form early publication.

#### Step 8: Request for examination

The patent application is examined only after receiving request for examination that is RFE.  Up on receiving this request the controller gives your patent application to a patent examiner who examinees the patent application with different patentability criteria like:

* Patentable subject matter
* Novelty
* Non-obviousness
* Inventive step
* Industrial application
* Enabling

#### Step 9: respond to objections

Majority of patent applicants will receive some type of objections based on examination report. The best thing to do it analyze the examination report with patent professional (patent agent) and creating a response to the objections raised in the examination report. This is a chance for an inventor to communicate his novelty over prior arts found in the examination report. The inventor and patent agent create and send a response to the examination that tries to prove to controller that his invention is indeed patentable and satisfies all patentability criteria’s.

#### Step 10: clearing all objections

This communication between controller and patent applicant is to ensure that all objections raised in the patent application are resolved. (if not the patent will not be granted ) and the inventor has his fair chance to prove his point and establish novelty and inventive step over existing prior arts.

#### Step 11: Grant of patent

The application would be placed in order for grant once it is found to be meeting all patentability requirements. The grant of patent is notified in the patent journal which is published time to time.