UNIT 4

Security Policies

- In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets.
- A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change.
- A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

Policies should define:

- Scope - Who the policy applies to.
- Who does the actions defined by the policy.
- Defines when defined actions are to be done.
- Defines where or on what equipment the policy applies to.
- Defines the organizational level that the policy applies to such as a division or the entire enterprise.
- Who enforces the policy
- What are the consequences of failure to follow the policy.
- Policies may reference procedures that are used but do not define the procedures. For example the policy may specify that passwords must be changed every 60 days but not provide a procedure telling how to change them.

Why Policies should be developed

- 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.

Security policy functions

- Protect people and information
- Set the rules for expected behaviour by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, probe, and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation

Email policy

- Electronic mail (e-mail) has become a ubiquitous service greatly enhancing communication both internally within a community and externally to Users
- The purpose of this policy is to describe the appropriate use of E-mail Facilities, associated responsibilities, and rights of all Users

www policy

- The World Wide Web is becoming an increasingly important information resource. It permits both institutions and individuals to access and distribute text and graphical information worldwide.
- www Policy is intended to promote use of the Internet as a publishing medium by clarifying the responsibilities of authors.
- It usually contains:
  - Guidelines applying to any web site housed on an enterprise-controlled server.
  - Guidelines for Administrative Web Sites
  - Guidelines for Non-administrative Web Sites

Email Security policies

- Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.
- The purpose of this email policy is to ensure the proper use of email system and make users aware of what deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Network.
- This policy covers appropriate use of any email sent from a email address and applies to all employees, vendors, and agents operating on behalf of .

Need of Email Policy

1. Protect against email threats: An email policy helps prevent email threats. A well laid out email policy makes your staff aware of the corporate rules and guidelines, which if followed will protect your company against (spear) phishing attacks and confidentiality leaks, aid compliancy and minimize legal liability.

2. Avoid misconduct: An email policy can help stop any misconduct at an early stage, for instance by asking employees to come forward as soon as they receive an offensive email. Keeping the incidents to a minimum can help avoid legal liability.

3. Reduce liability: If an incident does occur, an email policy can minimize the company's liability for the employee's actions. Previous cases have proven that the existence of an email policy can prove that the company has taken steps to prevent inappropriate use of the email system and therefore can be freed of liability.

4. Educate Email Etiquette: You can use your email policy to educate your employees in email etiquette to ensure that your company conveys a professional image in its email communications.

5. Warn employees of email monitoring: If you are going to use email filtering software to check the contents of your employees' emails, it is essential to have an email policy that warns your employees that their emails might be monitored.

Policy Review Process

The purpose of the review is to determine whether:

- the objectives of the policy or procedure are being achieved
- any amendments to the policy or procedure are required
- the policy or procedure should continue to apply or be disestablished.

To ensure the accuracy and completeness of whatever it is you're reviewing and to make sure everyone has the same understanding of the policy, process, or situation.

Corporate policies

- 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.

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

Sample security policy

I. The World-Wide Web is a powerful new medium of communication and a valuable resource to many members of the University community. This policy establishes guidelines for its use with two purposes in mind: to ensure free, fair access to and responsible use of the Web by the University community at large, and to establish an "official'' University presence on the Web through a consistent, clearly identifiable set of Web pages administered by the Office of Public Relations.

II. General Web Use. Any individual or group with authorized access to a University-owned computer or computer network may use it to gather information from and disseminate information via the World-Wide Web freely subject to the terms of this policy, other applicable University policies, and state and federal laws. Applicable University policies include, but are not limited to:

Academic Freedom

Academic Responsibility

Code of Ethics for Computing

Policy Concerning Harassment

Trademark Policy Statement

Joint Statement on Rights and Freedoms of Students

Academic Integrity

The standards of conduct for students

Sample security policy

- **III. Official University Web Pages.** The University's official presence on the Web is through a set of Web pages administered by the Office of Public Relations. Only these official Web pages are permitted to display facsimiles of the registered University seal, the University logo, or any of the official University print publications listed in Appendix A of the *Faculty and Contract Staff Handbook*, except by permission of the Office of Public Relations.

  Upon request, direct links will be provided from the official University Web pages to Web pages maintained independently by individual departments, divisions, and University offices listed in the University Administrative Structure chart in the *Faculty and Contract Staff Handbook*, and sponsored student organizations as defined in the *Student Handbook*. Direct links to Web pages maintained independently by individual faculty members, recognized student organizations, or other individuals or groups may be provided at the discretion of the Office of Public Relations.

  IV. Any violation of the provisions of Section II of this policy is necessarily a violation of an existing University policy and will be addressed through the procedures provided therein. The Office of Academic Affairs has the authority to restrict or prohibit Web use which it believes to be in violation of any provision of this policy on a temporary basis, until appropriate procedures resolve the matter. The Office of Public Relations has the authority to determine whether Web use is in violation of the provisions of Section III of this policy and to restrict or prohibit such use.

Publishing and Notification Requirement of the Policies

- The notification you received should contain details regarding the policy issue and an example page on which we found the issue.
- Read the notification carefully and make any appropriate changes to your site to resolve the issue. Sometimes it can be resolved by removing violating content or removing Google ads from those pages. In other cases, it may require changing the implementation of your ads.
- Keep in mind that the example page we provide is just an example, and you should review your entire site to ensure that the same issue doesn't continue to exist on other pages.

Information Security Standards

- The term "standard" is sometimes used within the context of 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.")

ISO

- ISO, founded in 1947, is a worldwide federation of national standards bodies from some 100 countries, with one standards body representing each member country. The American National Standards Institute (ANSI), for example, represents the United States. Member organizations collaborate in the development and promotion of international standards. Among the standards the ISO fosters is Open Systems Interconnection (OSI), a universal reference model for communication protocols.

- ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards.

- It is made up of our 162 member countries who are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland

What are standards?

- International Standards **make things work**. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency. They are instrumental in facilitating **international trade**.
- ISO has published more than 19 500 International Standards covering almost every industry, from technology, to food safety, to agriculture and healthcare. ISO International Standards impact everyone, everywhere

IT Act

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the *United Nations Model Law on Electronic Commerce 1996*

- The original Act contained 94 sections, divided in 19 chapters and 4 schedules. 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.

- The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formation 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.

- The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies

Copyright Act

- **Copyright** is a legal right created by the law of a country that grants the creator of an original work exclusive rights to its use and distribution, usually for a limited time. The exclusive rights are not absolute; they are limited by limitations and exceptions to copyright law, including fair use.
- Copyright is a form of intellectual property, applicable to any expressed representation of a creative work. Under US copyright law, however, legal protection attaches only to *fixed* representations in a tangible medium. It is often shared among multiple authors, each of whom holds a set of rights to use or license the work, and who are commonly referred to as rightsholders.These rights frequently include reproduction, control over derivative works, distribution, public performance, and "moral rights" such as attribution

A copyright notice should contain all the following three elements:

- The symbol © (the letter C in a circle), the word "Copyright" or the abbreviation "Copr."
- The year when the work was first created.
- The name of the owner of the copyright.
- **Example: © 2005 John Doe**

Patent Law

- A **patent** is a set of exclusive rights granted by a sovereign state to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an 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.
- 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 that define the invention. A patent may include many claims, each of which defines a specific property right. These claims must meet relevant patentability requirements, such as novelty, usefulness, 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

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, copyright and trademarks, 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.
- IP protection is intended to stimulate the creativity of the human mind for the benefit of all by ensuring that the advantages derived from exploiting a creation benefit the creator. This will encourage creative activity and allow investors in research and development a fair return on their investment.
- 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 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 CRIMES

- Cyber terrorists usually use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information.
- Internet is one of the means by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling illegal articles, pornography etc. this is done through many methods such as phishing, spoofing, pharming, internet phising, wire transfer etc. and use it to their own advantage without the consent of the individual.

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.

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.

Copy Right Law

- 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 author of a work is generally considered as the first owner of the copyright under the Copyright Act 1957. However, for works made in the course of an author's employment under a "contract of service" or apprenticeship, the employer is considered as the first owner of copyright, in the absence of any agreement to the contrary.

Software License

- A **software license** is a legal instrument (usually by way of contract law, with or without printed material) governing the use or redistribution of software. Under United States copyright law all software is copyright protected, except material in the public domain. A typical software license grants an 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 under copyright law.

- In addition to granting rights and imposing restrictions on the use of software, software licenses typically contain provisions which allocate liability and responsibility between the parties entering into the license agreement. In enterprise and commercial software transactions these terms often include limitations of liability, warranties and warranty disclaimers, and indemnity if the software infringes intellectual property rights of others.

- Software licenses can generally be fit into the following categories: proprietary licenses and free and open source. The significant feature that distinguishes them are the terms under which the end-user may further distribute or copy the software.

Software License (cont..)

- Software licenses typically are either proprietary, free or open source, the distinguishing feature being the terms under which users may redistribute or copy the software for future development or use.
- Software licenses typically provide end users with the right to one or more copies of the software without violating copyrights. 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 of the software, the limitations of liability, warranties and disclaimers and protections if the software or its use infringes on the intellectual property rights of others.

Semiconductor Law

- The **Semiconductor Chip Protection Act of 1984** (or **SCPA**) is an act of the US Congress that makes the layouts of integrated circuits legally protected upon registration, and hence illegal to copy without permission.

- The SCPA does not protect functional aspects of chip designs. That is reserved to patent law. Although EPROM and other memory chips topographies are protectable under the SCPA, such protection does not extend to the information stored in chips, such as computer programs. Such information is protected, if at all, only by copyright law.

Patent Law

- The history of Patent law in India starts from 1911 when the Indian Patents and Designs Act, 1911 was enacted. The present Patents Act, 1970 came into force in the year 1972, amending and consolidating the existing law relating to Patents in India. The Patents Act, 1970 was again amended by the Patents (Amendment) Act, 2005, wherein product patent was extended to all fields of technology including food, drugs, chemicals and micro organisms

Procedure for Grant of a Patent in India

- After filing the application for the grant of patent, a request for examination is required to be made for examination of the application by the Indian Patent Office.
- After the First Examination Report is issued, the Applicant is given an opportunity to meet the objections raised in the report.
- The Applicant has to comply with the requirements within 12 months from the issuance of the First Examination Report.
- If the requirements of the first examination report are not complied with within the prescribed period of 12 months, then the application is treated to have been abandoned by the applicant.
- After the removal of objections and compliance of requirements, the patent is granted and notified in the Patent Office Journal.