1. Introduction to Information Security Policies

Information Security Policy /ISP/ is a set of rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. An ISP is governing the protection of information, which is one of the many assets a corporation needs to protect.

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.

2. Purpose of Information Security Policies

Institutions create ISPs for a variety of reasons:

- To establish a general approach to information security
- To detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications.
- To protect the reputation of the company with respect to its ethical and legal responsibilities.
- To observe the rights of the customers; providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective.

3. Scope of Information Security Policies

ISP should address all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties in a given organization, without exception. Information Security policy is intended to support the protection, control and management of the organization's information assets. These policies are required to cover all information within the organization which could include data and information that is :

- Stored on databases
- Stored on computers and
- Transmitted across internal and public networks
- Printed or hand written on paper, white boards etc.
- Sent by facsimile (fax), telex or other communications method
- Stored on removable media such as CD-ROMs, hard disks, tapes and other similar media
- Stored on fixed media such as hard disks and disk sub-systems
- Held on film or microfiche
- Presented on slides, overhead projectors, using visual and audio media
- Spoken during telephone calls and meetings or conveyed by any other method

4. Why ISP is important.

- Minimizes risk of data leak or loss.
- Protects the organization from "malicious" external and internal users.
- Sets guidelines, best practices of use, and ensures proper compliance.
- Announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.
- Promotes proactive stance for the organization when legal issues arise.
- Provides direction to upgrade security standards internal or external to the organization.

5. What are the key objectives of any ISP.

Information security is deemed to safeguard three main objectives:

- **Confidentiality** – data and information assets must be confined to people authorized to access and not be disclosed to others;
- **Integrity** – keeping the data intact, complete and accurate, and IT systems operational;
- **Availability** – an objective indicating that information or system is at disposal of authorized users when needed.

Donn Parker, one of the pioneers in the field of IT security, expanded this threefold paradigm by suggesting also "authenticity" and "utility".

6. When and how policy is developed ?

By definition, the policy is the high-level document that's used to guide the formulation of procedures and guidelines. The policy answers the question of "What should be done and by whom?" The procedures and guidelines answer the question of "How should it be done?" Below are some tips for developing a comprehensive enterprise security policy. It's a checklist for any policy wonk given the responsibility of putting the document together.

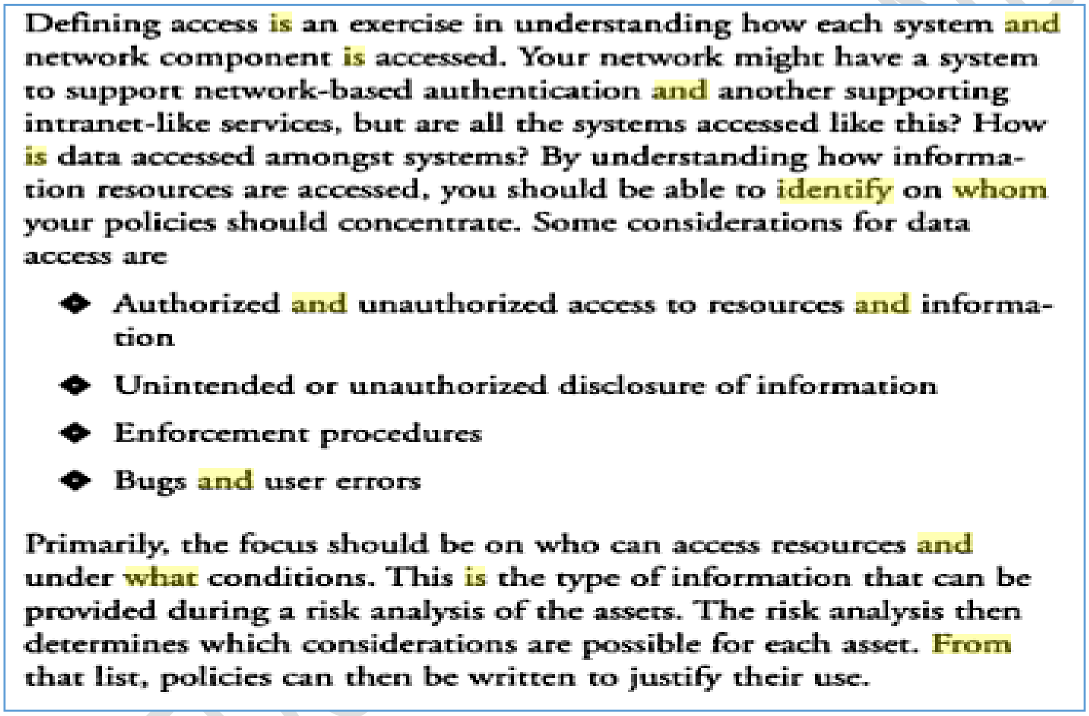
- Know your organization.
- Define the scope and the agenda.
- Know your target audience.
- Stay high-level, general and broad.
- Ensure that it can be easily translated to procedures and guidelines by the appropriate areas.
- Keep weaknesses and organizational deficiencies in mind
- Be aware of external drivers.
- Be realistic.
- Ensure version control and backups.
- Avoid controversy.
- Wear a white hat.
- Finally, don't forget to smile and keep your sense of humor.

7. Who will use your security policy ?

Your audience is of course all your company employees, but this group can be divided into audience sub-categories, with the members of each sub-category likely to look for different things from information security policy. The main audiences groups are:

- **Management** – all levels
- **Technical Staff** – systems administrators, etc
- **End Users -** All users will fall into at least one category (end-user) and some will fall into two or even all three.

8. Identify what and from whom it is being protected ?



Defining access is an exercise in understanding how each system and network component is accessed. Your network might have a system to support network-based authentication and another supporting intranet-like services, but are all the systems accessed like this? How is data accessed amongst systems? By understanding how information resources are accessed, you should be able to identify on whom your policies should concentrate. Some considerations for data access are

- Authorized and unauthorized access to resources and information
- Unintended or unauthorized disclosure of information
- Enforcement procedures
- Bugs and user errors

Primarily, the focus should be on who can access resources and under what conditions. This is the type of information that can be provided during a risk analysis of the assets. The risk analysis then determines which considerations are possible for each asset. From that list, policies can then be written to justify their use.

9. Data security consideration – Backups, Archival ?

A. Data handling

- Policies: how data is handled and how to maintain integrity and confidentiality of data
- Existence of third party data
- Personal data
- Personnel data
- Privacy protection
- COTS (Commercial Off-The-Shelf) software licensing

B. Backups

- Which data to back up
- Frequency of backups
- Revision of backup procedures

- On-site vs. Off-site storage of data

C. Archival Storage of Backups

- Retention period
- Readability assurance
- Media life time < retention period

D. Disposal of Data

- Dumpster diving
- Analysis of old hard drives

E. Intellectual Property Rights and Policies

- Who owns the rights to IP
- Interaction with documents under IP control
- Labeling for IP enforcement

F. Incident Response and Forensics

- Single point of contact = Assignment of responsibilities
- Procedures

10. Intellectual Property Rights and Policies and why do you need them ?

Intellectual property rights encourage innovation and discovery. The purpose of such rights is to give the legal owner of an invention or creative idea the exclusive opportunity to profit from it for a specified length of time. This means that the legal owner has the right to use the invention for personal profit and control how (or if) others can use it. Intellectual property rights arise from four basic sources. Each type has different requirements for acquiring the right in the first place, for protecting it over time, and for keeping others from infringing on it. The four basic sources of these rights are:

Patents: Used to protect inventions such as machines, processes, and designs for a stated length of time. A patent is an intellectual property right granted by U.S. federal law.

Copyrights: Used to protect art, music, videos, computer programs, books, and similar creative works for a stated length of time. A copyright is protected by U.S. federal law.

Trademarks: Used to protect words, symbols, and logos used to depict or identify a product or service, and protects them for as long as the mark is in use. Trademarks can be protected under both U.S. federal law and some state laws.

Trade secrets: Used to protect processes, methods, and formulas that must be kept secret to give an organization a competitive edge (think of the "Coca Cola secret formula"). Trade secrets can be protected under federal and state law. The most important concept for this type of intellectual property is that it remains secret.

- There are a number of best practices that a company, whether operating domestically or internationally should adopt:
- Employees and vendors must be required to sign a code of conduct and confidentiality, and non-disclosure agreements before beginning work.
- Electronically stored confidential information should be compartmentalized and accessible only on a need-to-know basis.
- Immediately revoke a departing employee's ability to access any proprietary information.
- Conduct an exit interview with the employee and require him or her to attest that he or she is not taking any confidential or proprietary information to a new employer.
- If suspicious activity on the part of the departing employee is uncovered, consider conducting a full-scale investigation of the former employee's recent conduct.

11. Role of Information Security Department ?

A. Data Steward

The enterprise vice-president or top-level executive having policy-level responsibility for a particular set of information assets. The Data Steward will:

- Establish standards for business use of information.
- Assign administrative responsibility to Business Owners.
- Monitor compliance and periodically review violation reports.

B. Information Security Committee (ISC)

The Information Security Committee is responsible for governance and oversight of the enterprise information security program. The ISC will:

- Analyze and manage institutional risks.
- Review and recommend policies, procedures, and standards.
- Ensure consistency in disciplinary processes for violation.

C. Chief Information Security Officer

The official responsible for directing implementation of the enterprise information security program. The Chief Information Security Officer will:

- Coordinate the development and maintenance of information security policies and standards.
- Investigate security incidents and coordinate their resolution as defined in the IT Security Incident Escalation Policy.
- Assist Business Owners in assessing their data for classification as defined in the Institutional Data Access Policy and advise them of available controls.
- Implement an information security awareness program.
- Serve as liaison to the Information Security Committee, law enforcement, Internal Audit, and University Legal Services.
- Provide consulting services for information security throughout the enterprise.

D. Data Custodian

The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms. The data custodian may or may not be IT staff.

E. Authorized User

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users will:

- Seek access to data only through the authorization and access control process.
- Access only that data which s/he has a need to know to carry out job responsibilities.
- Disseminate data to others only when authorized by the Business Owner.
- Report access privileges inappropriate to job duties to the Business Owner for correction.
- Attend training in security and confidentiality policies/procedures.

----

12. Establishing Type of Viruses Protection ?

A firewall – this acts as a gatekeeper to protect your computer from incoming attacks from the internet, by monitoring and filtering data traffic leaving and arriving on your computer.

Antivirus software – this helps to protect against viruses, trojans and other security threats by scanning and stopping viruses being installed on your computer. If you do get a virus installed on your PC, anti-virus software will be able to remove it.

Antispyware software – spyware is malicious software that secretly downloads to your computer. Once installed, it can monitor your activity, collect information about you and send it out onto the internet, and even take over your web browser (called ‘hijacking’). Anti-spyware software scans your computer to detect this, and removes any spyware it finds. By keeping anti-spyware software running, it can prevent spyware from being installed in the first place.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication

13. Handling third party software ?

- Identify reputation of the software based on history of operation.
- Use the third party software in accordance to the organizational security and intellectual property policy.
- Monitor the license agreement and report violations if any.
- Assess the risk of using the third party software.
- Talk to your stakeholders and request the necessary knowledge to use and deploy third party components.

----

14. How to maintain security policies ?

Standardize: Together, ISO 27001 and ISO 27002 represent the most comprehensive set of best practices for data security in a business environment.

PDCA: Plan-do-check-act (PDCA) protocol is the cornerstone of ISO 27001 standards. Working towards ISO 27001 certification is a worthy goal for any facility. Even if your organization doesn't require certification, PDCA is an important litmus test for any data security policy.

Auditing: Regular auditing of your security practices will ensure business rules are being implemented properly by all team members frequent or ongoing audits will ensure that both letters and the spirit of your security policies are being fulfilled on a daily basis.

Identifying Assets: Identifying your assets is the first step to developing an advanced security posture.

Back-up: Requirements for backing up data vary according to industry.

Access Control: Part of identifying and prioritizing your security assets involves assigning and maintaining access levels among staff.

Encryption: ISO 27002 standards dictate that a company-wide encryption policy is designed and implemented, covering standards and responsibilities for digital signatures, keys, certificates and any other encryption tools.

Real Time Monitoring: Threats against your network are constantly evolving. The best way to maintain a vigilant security posture is by implementing SIEM tools that keep track of logged data and correlate information from different sources, indentifying malicious behavior and giving your IT team tools/data to respond to emerging threats.

Log Collection and scalability