

Secure System planning & administration.

A system security plan is primarily implemented in organizational IT environments. It can be a proposed plan to protect & control an information system, or a plan to protect & control an information system that is already in implementation. It is usually created using the organization IT environment security policy as the benchmark.

- The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.
- Administration is defined as the activities of groups co-operating to accomplish common goals or the group of individual who are in charge of creating and enforcing rules & regulations, or those in leadership positions who complete important tasks.
- The basic functions of administration is, planning, Organising, Directing and Controlling.
- Typically a system security plan includes

- list of authorized personal users that can access the system
- level of access or what each user is allowed and not allowed to do on the system
- Access control methods, or how users will access the system (user ID / password, digital card, biometrics)

Orange Book

The Orange book standards are used to evaluate the security of both standalone and nw os. The current version of this publication date from 1985.

- The Orange book which was named for its Orange cover. It is a part of Series of Computer System Security guidelines & standards that are known as 'Rainbow Series'.
- Example:-
Microsoft windows Server, Server Configurations with C₂ (controlled Access protection) C₂ security standards outlined in the Orange book
- C₂ is one of a family of security designations that the Orange book applies to Computer Systems, which includes the following

- D (Minimal protection)
- C₁ (Discretionary Security protection)
- C₂ (Controlled Access protection)
- B₁ (Labelled Security protection)
- B₂ (Structured protection)
- B₃ (Security Domains)
- A₁ (Verified Design)

Security planning policy Requirements :-

Security policy requirements are consists of

- Confidentiality
 - * integrity
 - * Availability
- Confidentiality
 - It is a requirement whose purpose is to keep sensitive information from being disclosed to unauthorized receipts
 - Ex:- Defence, Banking
- Integrity:-
 - It is a requirement want to ensure that information & programs are changed only in a specified & authorized manner
 - It may be important to keep data consistent or to allow data to be changed only in an

approved manner

Ex:- withdraws from a bank account

→ Availability:-

It is a requirement intended to ensure that systems promptly & service is not denied to authorized users.

Accountability:-

→ Accountability is the acceptance of responsibility for one's own actions. It implies a willingness to be transparent, allowing others to observe and evaluate one's performance

→ It is taking or being assigned responsibility for something that you have done or something that you are supposed to do.

Example:-

when an employee admits an error she made on a project

→ It eliminates the time and effort you spend on distracting activities & other unproductive behaviour. When you make people accountable for their actions, you are effectively teaching them to value their work

when done right, it can increase your team member's skills and confidence

RED Book

→ The RED book was published to provide subsidiary information to enable the Orange book principles to be applied in a network environment. The RED book was initially published as the Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria.

→ Services in the RED book :-

- Communication integrity
 - * Authentication.
 - * Communication field integrity
 - * Non - Repudiation

→ Denial of Service

- * Continuity of operation
- * protocol-based protection
- * Network - management

→ Compromise protection

- * Data Confidentiality
- * Traffic Confidentiality

→ Other Security Services in the RED book.

→ Describe Services

- * functionality
- * Strength : how well it is expected to meet its objective

* Assurance :-

derived from theory, testing, practices validation and verification

→ Rating

- * None
- * medium
- * minimum(1)
- * Fair
- * Good (B₂)
- * Not offered - present

→ Acceptance of these criteria has grown to the extent of that some commercial companies require their purchases to satisfy a specific level of security as described in the orange & Red books

Government Network Evaluation :-

The purpose of the evaluation:-

- Evaluation :- assessing whether a product has the security properties claimed for it
- Certification :- assessing whether a product is suitable for a given application.
- Accreditation :-

deciding that a product will be used in a given application.

- * Independent verification & validation by an accredited & competent & trusted third party
- * provides a basis for international certification against specific formal standards by national

Information Security policies and procedures

Security policies are living documents that are continuously updated and changing as technologies, vulnerabilities and security requirements change.

Physical security policies

Sensitive buildings, rooms and other areas of an organization.
• who is authorized to access, handle and move physical assets.

Responsibilities of individuals for the physical assets they access and handle.

Information security policies

⇒ Confidentiality

⇒ Integrity

⇒ Authentication

⇒ Availability

⇒ Utility

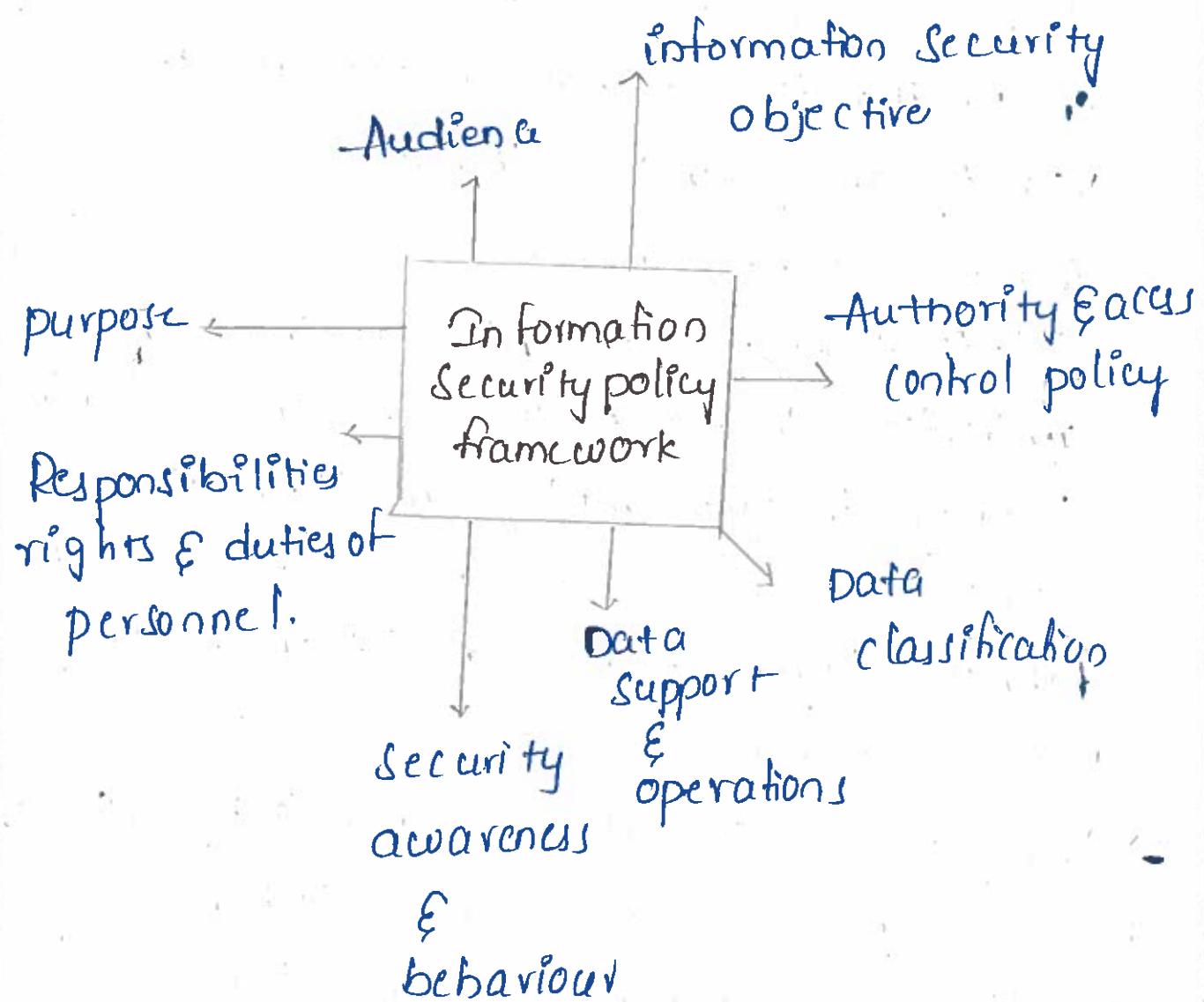
Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges.

Security procedures :-

Security procedures are detailed step-by-step instructions on how to implement, enable, or enforce security controls as enumerated from your organization's security policies. Security procedures should cover the multitude of hardware and software components supporting your business processes as well as any security related business processes themselves.

Information Security Policies & Procedures.

An information security policy (ISP) sets forth rules & processes for workforce members, creating a standard around the acceptable use of the organization's IT including networks & applications to protect data confidentiality, integrity and availability.



→ It means the state of being responsible or answerable for a system, its behaviour & its potential impacts. It is an acknowledgement of responsibility for actions, decisions & products. Responsibility can be legal or moral (ethical).

Network Security

- Network Security is a set of technologies that protect the usability & integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats.
- A nw security architecture is composed of tools that protect the nw itself & the applications that run over. It effective nw security strategies employ multiple layers of defense that are scalable and automated. Each defensive layer enforces a set of security policies determined by the administrator.
- Simply, it is a set of rules and configurations designed to protect the integrity, confidentiality & accessibility of computer networks & data using both software & hardware technologies.

Authorities

Targets of the Evaluation :-

- * products eg:- os, which will be used in a variety of applications & have to meet the generic security requirements
- * systems, i.e a collection of products assembled to meet the specific requirements of a given application.

Structure of the evaluation criteria :-

- functionality :- the security features of a system eg:- DAC, MAC, authentication, auditing
- Effectiveness :- The mechanisms used appropriate for the given security requirements

Assurance :-

The thoroughness of the evalution.

Organizations of the evaluation process :-

* Government agency :-

backs the evaluation process & issues the certification

* Accredited private enter prize :-

enforce the consistency of evaluations
(repeatability and reproducibility)

Method of the Evaluation :

A method must prevent from product -

Oriented & process-oriented

product-oriented

* Examine & test the product

* Different evaluations may give different results

Process-oriented

* process of product development

Costs of evaluation

→ Costs:-

* Free paid to evaluation

* Time to collect required evidences

* Time & money of training of evaluators

* Time & efforts of liaising with the evaluation team.