2 Policies

2.1 Security Policies

2.1.1 The Nature of Security Policies

2.1.2 Types of Security Policies

2.1.3 The Role of Trust

2.1.4 Example: Academic Computer Security Policy

2.2 Confidentiality Policies

2.2.1 The Bell-LaPudala Model

2.3 Integrity Policies

2.3.1 The Biba Model

2.4 Availability Policies

2.4.1 Goals of Availability Policies

2.4.2 Denial of Service Models

2.4.3 Example: Availability and Network Flooding

Practical Works

Visit an organization in your local place and develop security policies and procedures for that organization. Present the prepared report in front of your classmates and the stakeholders of that organization.

What is a security policy?

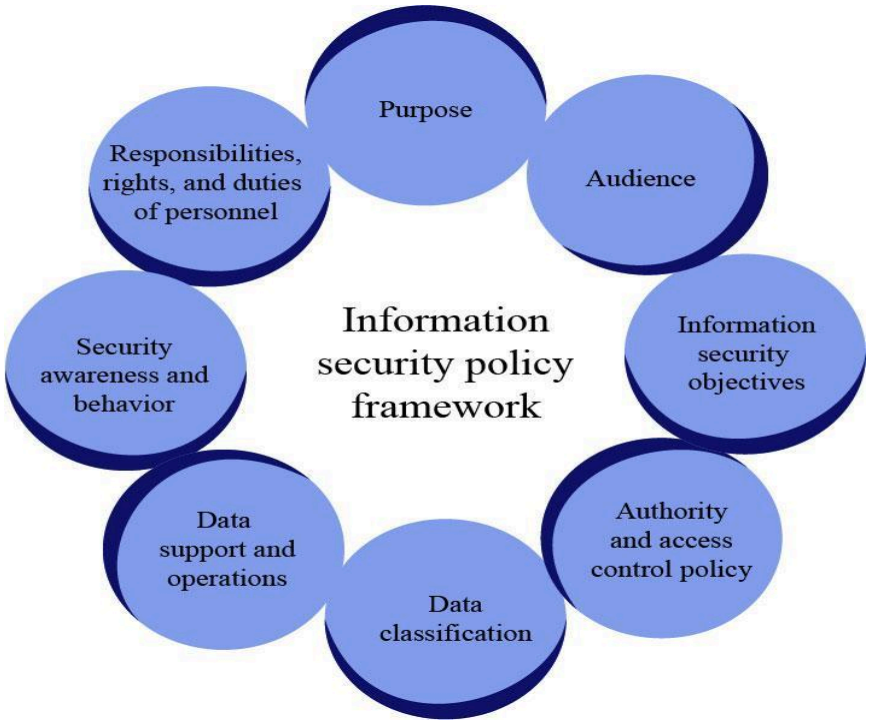
By definition**, security policy refers to *clear, comprehensive*, and *well-defined* plans, rules, and practices that regulate access to an organization's system and the information included in it. Good policy protects not only information and systems, but also individual employees and the organization as a whole**. It also serves as a prominent statement to the outside world about the organization's commitment to security.

A security policy (also called an information security policy or IT security policy) is a document that spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data. Security policies exist at many different levels, from high-level constructs that describe an enterprise's general security goals and principles to documents addressing specific issues, such as remote access or Wi-Fi use..

A security policy is frequently used in conjunction with other types of documentation such as standard operating procedures. These documents work together to help the company achieve its security goals. The policy defines the overall strategy and security stance, with the other documents helping build structure around that practice. You can think of a security policy as answering the "what" and "why," while procedures, standards, and guidelines answer the "how."

Nature of security policy

There are 8 elements of security policy



Nature of security policy

1. Purpose

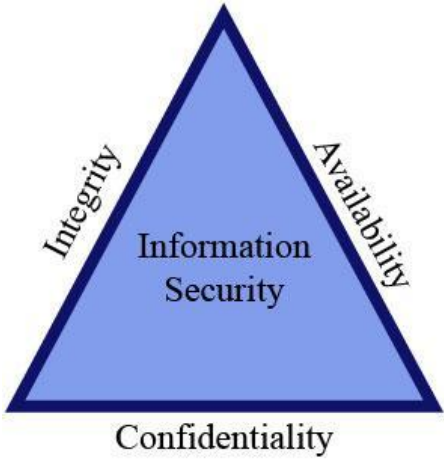
The purpose of security policy is to create the approach of information security. It detects the information security threats such as misuse of networks, applications, software, computer systems. It maintains the reputation of organizations and legal responsibilities. The main purpose is to respect the customer and aims to fulfill customer requirements.

2. Audience

It defines the audience to whom the IT security policy applies and identifies those audiences which are out of the scope of the computer security policy. It defines customer requirements and statements also.

3. Information security objectives

Information security is a set of tools used to protect the digital and analog information. Its protection covers a range of IT domains as well as computer security. The main guideline of information security policy is to use tools like authentication and permissions to restrict an unauthorized user from accessing private and sensitive information. This protection helps to prevent information theft and modification or loss. The security measures of ISP consist of three main objectives also known as CIA.



a. Confidentiality

Confidentiality ensures the protection of secret and sensitive information from unauthorized users. It is a key feature of cybersecurity policy also. It uses multi-factor authentication, encryption, strong password, and segregation of data to maintain the access restriction. Security breaches of confidentiality occur due to human error or malicious event. It also protects from third-party software.

b. Integrity

In The world of security policy, Integrity defines the completeness and accuracy of the data. Integrity is important so that no one can modify the data and no one can misuse the data. Integrity ensures that the consistency and trustworthiness should be maintained over the whole life cycle. It also involves that during

the transmission of data the data should remain unchanged. And, all the precautionary steps should be taken by the organization so that unauthorized user cant have an access of the confidential data.

c. Availability

Availability ensures that authorized users can reliably access the information. It is maintained through continuity of access procedures, backup, and duplication of information. It ensures the maintenance of hardware and network connections as well. When the network is attacked due to natural disasters, or when client devices fail, this situation is called the loss of availability.

4. Authority and access control policy

This element follows the hierarchical pattern. The security policy may have different terms for a senior manager, junior manager, or company employee. A senior manager may have the right to decide what data can be shared and with whom. Users have unique login IDs and credentials provided by the company which is used for the authentication of users.

5. Data classification

It classifies the data like top-secret data, secret data, confidential data, and public data. The objective of classifying data is to ensure that the sensitive data is protected from individuals and private data is protected from public access.

6. Data support and operations

It supports data backup, movements of data, and data protection. Data backup is necessary for security measures. To store backup media and move back up to the cloud for further procedure. Systems that store personal data or sensitive information must be protected according to industry compliance standards.

7. Security awareness and behavior

It provides training programs to educate the employees regarding security procedures and mechanisms. It follows three guidelines:

- Clean desk policy.
- Acceptable internet usage policy.

- Social engineering.

8. Responsibilities, rights and duties of personnel

It describes the responsibilities of company employees, appoints staff to carry out the user access reviews, comments, and manage security incidents. Responsibilities, rights, and duties are clearly defined as part of IT security. This is the most important requirement in Cyber security.

What is Zero Trust security?

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. ZTNA is the main technology associated with Zero Trust architecture; but Zero Trust is a holistic approach to network security that incorporates several different principles and technologies.

More simply put: traditional IT network security trusts anyone and anything inside the network. A Zero Trust architecture trusts no one and nothing.

Traditional IT network security is based on the castle-and-moat concept. In castle-and-moat security, it is hard to obtain access from outside the network, but everyone inside the network is trusted by default. The problem with this approach is that once an attacker gains access to the network, they have free rein over everything inside.

This vulnerability in castle-and-moat security systems is exacerbated by the fact that companies no longer have their data in just one place. Today, information is often spread across cloud vendors, which makes it more difficult to have a single security control for an entire network.

Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. This added layer of security has been shown to prevent data breaches. Studies have shown that the average cost of a single data breach is over $3 million. Considering that figure, it should come as no surprise that many organizations are now eager to adopt a Zero Trust security policy.

Types of security policy

The main types of security policies are:-
An organizational security policy- This security policy describes the organizations security policy as in whole and also defines its assurance to information security. One can understand it like a parent security policy. All the security policies are derived from this. It also defines the organizations goals.
System-specific security policies - this security policy mainly focuses on security policy of a particular system. the example of this can be :payroll system, data archive system and customer-facing application.
Issue-specific security policies- this type of security policy focuses on particular issues. such as Threat and categories of threat. For example, It may be possible that an organization has an implementation of security policy on phishing attacks only or some other category of threat.

Security policy examples

A large and complex enterprise might have dozens of different IT security policies covering different areas. The policies you choose to implement will depend on the technologies in use, as well as the company culture and risk appetite. That said, the following represent some of the most common policies:

1. **Program or organizational policy:** This high-level security blueprint is a must for all organizations, and spells out the goals and objectives of an information security program. The program policy also specifies roles and responsibilities, compliance monitoring and enforcement, and alignment with other organizational policies and principles.

2. **Acceptable use policy:** This is an issue-specific policy that defines the acceptable conditions under which an employee can access and use the company's information resources.

3. **Remote access policy:** This issue-specific policy spells out how and when employees can remotely access company resources.

4. **Data security policy:** Data security can be addressed in the program policy, but it may also be helpful to have a dedicated policy describing data classification, ownership, and encryption principles for the organization.

5. **Firewall policy:** One of the most common system-specific policies, a firewall policy describes the types of traffic that an organization's firewall(s) should allow or deny. Note that even at this level, the policy still describes only the "what"; a document describing how to configure a firewall to block certain types of traffic is a procedure, not a policy.

Confidentiality Policies

A confidentiality policy is intended to protect secrets; specifically, it is intended to prevent unauthorized disclosure of information. One *model* (general purpose template) of a confidentiality policy is the Bell–LaPadula (BLP) security model.

The Bell–LaPadula model leverages mandatory access control: the model does not give users power to alter access control in the system manifested in a principle called *tranquility*.

Multi-Level Security

Simplest form**, BLP** is a multi-level security model that protects Confidentiality. The goals of the system are to keep secrets with specific confidentiality *classifications* disclosed only to subjects with the appropriate *clearances* to read them. In addition, subjects should not be able to accidentally (or intentionally) leak secrets to other subjects with lower clearances.

In BLP, each subject S and object O is assigned a confidentiality level (L_S and L_O, respectively). The classification levels are:

Top Secret	(TS)
Secret	(S)
Confidential	(C)
Unclassified	(UC)

The most important, or most sensitive data are kept at the Top Secret (TS) level. Data that can be read by anyone is kept at the Unclassified level. The levels in between provide granularity so that some data can be shared in limited ways.

The **Simple Security Condition** requires that a subject S can *read* an object O only if $L_O \leq L_S$ and any DAC(Driver Authorization Card) permits it ("read down").

The **F-Property** requires that a subject S can *write* to an object O only if $L_S \leq L_O$ and any DAC permits it ("write up").

This means that in BLP, all subjects can tell their secrets to anyone with an equal or higher clearance and they can listen to secrets classified as their level or in a level less confidential. These rules are mandatory, and controlled by the system.

Formally: given a system with set of states Σ and set of transformations T that map from one state $\sigma_i \in \Sigma$ to another $\sigma_j \in \Sigma$, and an initial state σ_0: If the Simple Security Condition and F–Property are preserved by all $t \in T$ *and* σ_0 is secure, then the system is considered *secure*.

Integrity Policies

An integrity policy is intended to protect the trust in data, and not keep the data secret. Its primary purpose is to keep the quality of data as high as possible. At first glance, it seems that Confidentiality and Integrity policies are very similar but approach Security from different perspectives. In Confidentiality, the system is designed to protect how much everyone can trust *who accesses the data*. In Integrity models, the system is designed to protect how much everyone can trust *the origin or quality of the data*. One feels very much like read–access control and the other feels very much like write–access control.

Biba's Model

So how do we *maintain* integrity in a system and avoid this race to the bottom? Kenneth Biba probably saw how Integrity seems like the inverse of Confidentiality, so he turned the Bell–LaPadula model on its head and protect trust in the data and not in who accesses it.
In Biba's model, each subject S and object O is assigned an integrity level in I. Subjects can only create content *at or below* their integrity level and can view only at or above. His model effectively has the *inverse* principles to the Simple Security property and the F–property.

1. A subject s can only read an object o if $I_s \leq I_o$ ("read–up"; inverse of Simple Security).

2. A subject *s* can only write to an object *o* if $I_o \leq I_s$ ("write–down"; inverse of F–Property).

Colloquially: if you are trustworthy, you can tell untrustworthy subjects what you know. If you are untrustworthy, you can only listen to subjects at least as trustworthy as yourself (so you don't learn lies).

Availability Policies:

Goals of Availability Policies:

a. The purpose of this policy is to define requirements for proper controls to protect the availability of the organization's information systems.
b. Information systems must be consistently available to conduct and support business operations.
c. Information systems must have a defined availability classification, with appropriate controls enabled and incorporated into development and production processes based on this classification.
d. System and network failures must be reported promptly to the organization's lead for Information Technology (IT) or designated IT operations manager.
e. Users must be notified of scheduled outages (e.g., system maintenance) that require periods of downtime. This notification must specify the date and time of the system maintenance, expected duration, and anticipated system or service resumption time.
f. Prior to production use, each new or significantly modified application must have a completed risk assessment that includes availability risks. Risk assessments must be completed in accordance with the Risk Assessment Policy (reference (a)).
g. Capacity management and load balancing techniques must be used, as deemed necessary, to help minimize the risk and impact of system failures.

Denial of Service Models

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Example: Availability and Network Flooding

There are two general methods of DoS attacks: network flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular network flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.