

Information security: fundamentals:-

Employee responsibilities:-

The importance of the employee responsibility & there are 5 types.

1. Reveals your character
2. Helps secure your position
3. Show accountability.
4. Establishes trust
5. position you for advancement.

Reveals your character:-

Your responsibility for your work place and duties demonstrates your work ethic. Being a responsible employees show you take pride in your work place and about your worth. and also it view you as a dependable and self reliant employee and have faith in your abilities.

☀️ Helps secure your position :-
~~~~~

☀️ A responsible employee helps to provide the company with consistency and security.

☀️ And also your strong work ethic and dependable nature and demonstrative your value.

☀️ By assuming your responsibility at work, you become an asset to the organization and gain job security.

☀️ Because employers tend to keep employees who deliver the best work and show consistency in their behaviour.

☀️ Show accountability :-

☀️ Having accountability means that you accept that the consequences of your actions, whether they be good (or) bad.

☀️ workers who are accountable learn from their mistakes and become better because of them.

☀️ working to rectify your errors, and accepting praise for a job well done.

#### 4. Establishes trust:-

☺- Honesty when admitting an error and the moral character to cheer others on for their accomplishments helps to develop trust in the work place.

☺- Develop mutual respect with coworkers and supervisors to develop trust, credibility, and foster a healthy

● Company culture.

☺- positions you for advancement:-

☺- Responsibility is the most important in work place

● because a strong work ethic.

☺- Respect for others can impress your employer

and open up opportunities for the career advancement.

☺- And also mainly workers responsibilities are the:-

☺- Awareness.

☺- Integrity.

☺- Accountability.

## ☼ Tools of information security :-

☼ protecting our IT environment is very critical and also in every organization needs to take cyber security very seriously.

☼ There are number of hacking attacks which affecting business of all sizes.

☼ Hackers, malware viruses are some of the real security threats in the virtual world.

☼ There are 6 types in the cyber security tools and they are :-

☼ fire walls.

☼ Anti virus Software.

☼ PKI Services.

☼ MDR Services.

☼ penetration testing.

☼ Staff training.

## ☼. Fire wall<sup>o</sup> - ~ ~ ~ ~ ~

☼. As we know, the fire wall is the core of security.

☼. And it becomes one of the most important security tools.

Its job to prevent an authorized access to from a private NW.

☼. The fire wall is very useful, but it has limitation also.

A skilled hacker knew how to create data that are

believing like trusted fire walls.

## a. Anti virus software<sup>o</sup> - ~ ~ ~ ~ ~

☼. Anti virus software is a program which is designed to prevent, detect, and remove viruses and other malware attacks.

on the individual computer networks.

☼. And there are the variety types of NWs and they are:

- 1) Trojan horses
- 2) worms
- 3) key loggers
- 4) browser hijackers
- 5) spyware

☼- PKI Services -

~ o ~~~~~

☼- The Name PKI stands for public key infrastructure.

☼- This tool supports the distribution and identification of public encryption keys.

⊕ PKI can also be used to:

- Enable multi factor Authentication and Access control.

☼- Create compliant, trusted signatures like digital.

☼- Encrypt Email communications and authenticate the senders identity.

☼- Digitally sign and protect the code

## ☛ penetration testing:-

⇒ It is an important way to evaluate our business security systems and also IT infrastructure by safely trying to exploit vulnerabilities.

⇒ A pen test attempts the kind of attack business might face from the criminal hacker such as

☛ password cracking.

☛ code injection.

☛ phishing.

## 6. Staff training:-

☛ Staff training is not cyber security tool but ultimately having knowledgeable employees.

☛ who understand the cyber security which is the one of most strongest forms and defence against the cyber attacks.

#### 4. Managed Detection and Response Service (MDR) :-

☼- Today cyber criminals and hackers used for more advance techniques.

☼- Software to breach organization security so, there is necessity for every business to be used more powerful forms of defence of cyber security.

☼- The Managed Detection and Response has the following characteristics :-

- managed detection and response is focused on threat detection, rather than compliance.
- MDR relies heavily on security event management and advance analytics.
- while some automation is used, MDR also involves humans to monitor our network.

\* And also information processing can be classified into three stages.

And they are:-

\* Sensory memory.

\* Short-term memory

\* Long-term memory.

\* Sensory memory:-

And in the memory which can be divided into the sensory it is known as the sensory memory

\* Short-term memory:-

\* And the short term memory can be defined as the data which can be stored temporarily.

\* Long-term memory:-

The long term memory can be defined as the data which can be stored permanently.

Q. Information processing:-

⇒ Information processing can be defined as the processing of information in any manner detected by an observer.

⇒ As such, it is a process that describes every thing that happens in the universe, from the falling of a rock to printing text file in to digital computer system.

And in this information processing it has a cognitive theory.

Q. Cognitive theory:-

• This theory views the mind as a computer that accepts the inputs and also it performs the processing activities of those inputs.

## Security program management

☛ The Security program manager will be responsible for complete overview and driving security initiatives across product, engineering and business management.

⇒ The main purpose of Security program is the entity of an organization security policies, procedures, tools and controls.

⇒ Essentially, your security program is full, multi-faceted security strategy and governance that protects your organization's sensitive data and capabilities.

⇒ There are 5-types of security software your business needs

☛ Computer Antivirus

☛ N/w security.

☛ Fire walls.

☛ password managers.

And the information processing has the 4 types and they are:-

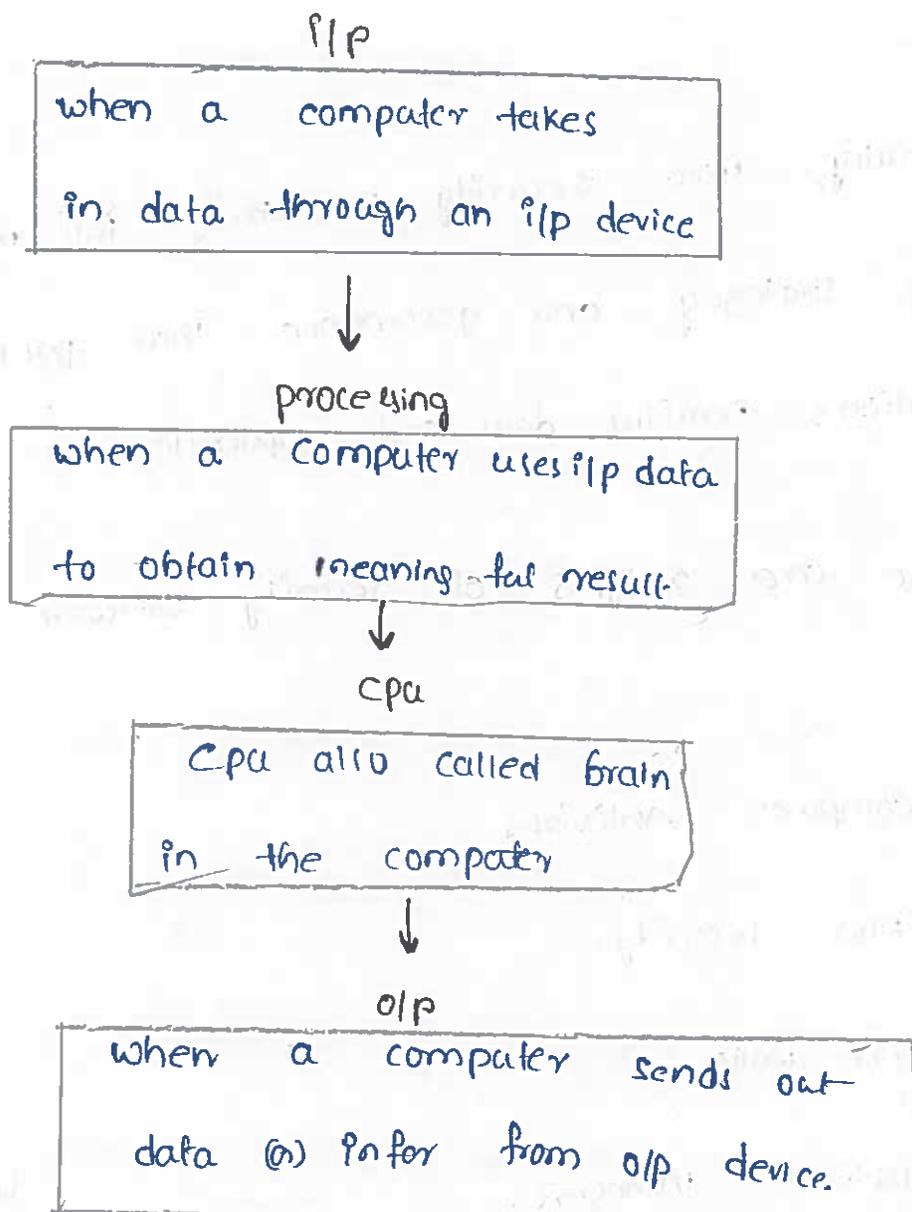
(i) Input

(ii) processing

(iii) cpu

(iv) output.

Block diagram of information processing cycle.



# Security Program Administrations

An effective security management process comprises six subprocesses.

⇒ policy

⇒ Awareness

⇒ Access

⇒ Monitoring

⇒ Compliance

⇒ Strategy.

## • Security Program Administration

⇒ In today's world, most business facilities some level of the site security.

⇒ Accordingly, the decision to manage security responsibilities in-house, (or) the selection of an external security administration partner.

⇒

## Trident Capabilities :-

- ⇒ As former 'top tier' special operations operators, Trident CING personnel have spent years in assessments governments and managing security and other assets.
- ⇒ As your SPA partner, Trident CING will review your existing security plan, set of improvements for consideration.
- ⇒ Trident CING will develop budgets covering security enhancements cooperate in the process, wherever the location.
- ⇒ Trident CING can provide security to meet any challenge.

## Information classification

Information classification is a process in which organisations assess the data that they hold and the level of protection it should be given.

● Organisations usually classify information in terms of confidentiality.

⇒ Confidentiality

⇒ Restricted

⇒ Internal

● ⇒ Public Information.

### Public Data :-

This type of Data is freely accessible to the public. It can be freely used, reused and redistributed without repercussions.

An example might be first and last names, job descriptions, or press releases.

## Internal-only data :-

This type of data is strictly accessible to internal company personals (or) internal employees who are granted access.

This might include internal-only memos, (or) other communications.

## Confidential data

Access to confidential data requires specific authorization and clearance. Types of confidential data might include social

security numbers, card holders data, MFA documents.

Usually confidentiality data is protected by laws like HIPAA and the PCI DSS.

# Information handling

Information handling is the process of gathering, analysing, reporting and presenting information.

It ensures the integrity of research data

• since it addresses concerns related to confidentiality, security, and retention of research data.

Proper planning for data handling can also result in efficient and economical storage,

• retrieval and disposal of data.

The two types of data handling are

- 1) qualitative data
- 2) quantitative data.

Qualitative data gives descriptive information of something whereas quantitative data gives numerical information about

Some thing. Data can be represented in various forms through the numbers.

## Types of Data Handling

Data can be represented in different types

- ⇒ Bar Graph
- ⇒ pictograph
- ⇒ Line Graph
- ⇒ stem and leaf plots
- ⇒ histogram
- ⇒ Dot plots
- ⇒ Cumulative Tables and graphs
- ⇒ Frequency Distribution.

It is also used for comparing data and taking out mean, median, and mode.

which is useful for both maths and science.