WHAT IS INFORMATION ASSURANCE?

The practice of **managing information-related risks** and the **needed steps that are involved to protect the information systems**.

The degree of confidence one has that **security measures protect and defend** the information and their systems.

Principles of Information Assurance

Confidentiality

- Protection against unauthorized access at all times.

Integrity

- Sensitive information is protected from unsanctioned modifications or deletions. Immutable data is never to be modified at any cost.

Availability

- Users with authorized access are granted a pass without bothering their activities.

Authentication

- Identifies all devices, users and applications that attempt access to protected information. These are validated to ensure that they are who they appear.

Nonrepudiation

- Those that are verified to access protected information or have been given access in any point in time should not be denied of any action as they are relative to the information.

WHAT IS INFORMATION SECURITY?

The practice that involves the protection of information by reducing risks.

Protection against;

Unauthorized access, Use, Disclosure, Disruption, Modification, or destruction.

10 commandments of Computer Ethics

1st Thou shalt not use a computer to harm other people.

2nd Though shalt not interfere with other people’s computer work.

3rd Thou shalt not snoop around in other people’s computer files.

4th Thou shalt not use a computer to steal.

5th Thou shalt not use a computer to bear false witness.

6th Thou shalt not copy or use proprietary software for which you have not paid.

7th Thou shalt not use other people’s computer resources without authorization.

8th Thou shalt not appropriate other people' intellectual output

9th Thou shalt think about the social consequences of the program you are writing or the system you are designing.

10th thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.