PRINCIPLES OF Cybersecurity

Cybersecurity is the practice of protecting information and the systems that process information. There are five primary principles associated with the discipline.

Confidentiality

Information has confidentiality if it can only be accessed and read by authorized users. Authorized users typically include the person generating the information and the intended recipients of the information.

Integrity

Information has integrity if it can only be modified by authorized users. Integrity should also be verifiable, meaning it should be easy to determine if information has been modified by an unauthorized third party.

Availability

Information is considered available if it can be accessed when and where it is needed. Access to information should also be timely and convenient for the user.

Non-repudiation

Non-repudiation deals with methods to link a user to actions taken by that user. For example, a person's signature on a legal contract can be used to prove the person agreed to the terms of the contract. It is difficult for the person who signed the contract to later deny or repudiate he did so.

Authentication

Authentication deals with positively identifying and verifying the identity of a user. This is a critical component to ensuring that only authorized users can access or modify information.