The CIA triad stands for Confidentiality, Integrity and Availability. It’s a model that guides policies of Information Security for an organization. Security experts consider the three elements of CIA as the most important components of security.

In the context of information security, confidentiality refers to a set of rules that limit your access to any piece of information. Integrity is an assurance of the information to be accurate and trustworthy. Availability refers to information access for authorized people.

**Confidentiality**

In information security, Confidentiality refers to information privacy. Measures to ensure confidentiality prevent malicious users from accessing sensitive information, while allowing authorized people to access it. It is a common practice to categorize data according to the type and amount of damage that can arise a result of it falling into the wrong hands.

In order to ensure data confidentiality, employees get information security trainings and learn the security risks that can cause a threat to the information. They learn how to guard against threats and familiarize themselves with risk factors. Other training aspects include knowledge of password best practices and social engineering techniques.

**Integrity**

Integrity includes maintaining the accuracy, consistency and trustworthiness of data during its lifecycle. It is to ensure that data remains the same and is without changes during transit. It also involves methods that ensure that any unauthorized people are unable to alter data. These methods are user access controls and file permission.

Moreover, version controls can help in preventing accidental deletion or changes from becoming a problem. To verify integrity, some data may also include checksums or cryptographic checksums. It’s also very important to keep a backup to restore any affected or changed data to its original state.

**Availability**

Availability in information security refers to data being available at all times by those who are authorized to access. One needs to maintain hardware or perform repairs whenever needed. You must also have a working operating system that is without any software errors. You also need to be updated with system upgrades, provide acceptable communication bandwidth and prevent bottlenecks from occurring.

It is also directly concerned with safeguard against data loss or interruption in the connection, along with unpredictable natural disasters such as floods and earthquakes. To guarantee the availability of information, you should always store a backup copy in a safe place. Software such as proxy servers and firewalls can help guard your systems against downtime.

Get comprehensive cyber security consultancy services of Aardwolf today to ensure overall security of your organization from all the three security aspects of confidentiality, integrity and availability!