**What is Information security?** – well, long answer short Information Security or InfoSec is about preventing unauthorized access to your system. Yes, that’s it…. well not truly, it’s not just that.

InfoSec’s primary focus is the protection of Confidentiality, Integrity and Availability, also referred to as CIA triad with efficient policy implementation using the AAA model (Authentication or authN, Authorization or authZ and Accounting or auditing)

In Short – InfoSec is ensuring there is **proper** data flow with focused implementation of CIA triad and AAA model.

Unpacking the “**proper**” data flow definition:

1. You cannot view data that you shouldn’t
2. You cannot change data that you shouldn’t, and
3. You can access data that you should.

These map directly with CIA triad.

|  |  |  |
| --- | --- | --- |
| You cannot view data that you shouldn’t | Only the right people can see the data | **Confidentiality** |
| You cannot change data that you shouldn’t | trust that data hasn’t been changed inappropriately | **Integrity** |
| You can access data that you should | able to get data when required | **Availability** |

Let’s take a data flow example and extend our CIA triad understanding further:

Since the new education system is all about online schooling. Let’s take an example of that. Consider that there is a Teacher-A who is accessing the School database for getting next week’s class schedule. Teacher-A can access the system and get the required data.

But a new challenger comes into the picture. It can be any hacker, alien or a naught school kid. They want to breach your security and access the system to:

1. Read or/and change Data at Rest
2. Eaves drop and tamper the Data in Transit
3. Disable your systems database, or block Teacher-A’s communication system overall.

So, security is about preventing such unauthorized access while maintaining data availability to the right people. In order to achieve this comes in picture the AAA model so as to maintain proper data flow.

1. Authentication (authN) – who are you?

This is an important aspect before the system lets any user to access the system without providing their identity. This includes Passwords, Multi Factor Authentication (MFA), or Single Sign On (SSO) from an external system.

1. Authorization (authZ) – what are you allowed to do?

This includes both reading and writing access. For example, as a student you can see the class schedule but cannot change it. That access of changing the schedule is with the Teachers or may be school coordinators only.

1. Accounting – what did you do or what happened?

This includes reading or writing data or even logging of information. For example, if a teacher looks up the personal details of a student’s guardian then that should be logged and the teacher can be held accountable that it’s for some valid reason only.

Let’s extend the same data flow example and understand how AAA model fits into this:

1. Teacher-A can access the system and get the required data but only when authenticates
2. Comes in the AuthN system, where the Teacher-A has to login and get an access token.
3. The AuthN system now talks to the accounting system and logs that Teacher-A did validate their identity successfully.
4. Now, the Teacher-A passes the access token to the school system.
5. The school system checks with AuthN system that the access token is indeed generated from there and then talks to AuthZ system to check whether Teacher-A is allowed to make that particular action of reading the class schedule.
6. Since Teacher-A is allowed the AuthZ responses with a success and then School system respnds success as well.
7. This data also gets recorded in the accounting system.

Now let’s bring the Ninja student in picture.

1. Ninja 1st tries to impersonate as Teacher-A and tries to login to the school system.
2. The AuthN system rejects the identity and denies the login attempt.
3. This also gets logged in the Accounting system as a failed login attempt for Teacher-A (since Ninja is impersonating Teacher-A)
4. Now, Ninja student uses its own credentials to login to School system which is approved by AuthN system and grants an access token, since Ninja knows its userID and password.
5. The successful login for Ninja is recorded in Accoutning system.
6. When Ninja asses the access token (login) the school system checks with AuthN system that the access token is indeed generated from there and then talks to AuthZ system to check whether Ninja is allowed to make that particular action.
7. If Ninja is making any other request apart from reading the schedule, like editing then AuthZ denies that request and logs it in the Accounting system as well.

That concludes the CIA triad and AAA model high level understanding. Security is a mindset and following the right principles like Least privilege, Defense in depth and Fail securely enables to implement that mindset.

Some references to read and understand this further:

1. [OWASP’s Security Design principles](1.%09https:/wiki.owasp.org/index.php/Security_by_Design_Principles)
2. [Information Security](https://en.wikipedia.org/wiki/Information_security)
3. [Public bucket breach](https://www.google.com/search?q=public+bucket+breach)