Access Control

Return to Glossary

Access Control is a security aspect that handles how user as well as system communicates and use resources. In order to enforce security, each and every access to the system and its resources should be controlled and should ensure only authorized access are allowed. This feature is mainly used to protect against unauthorized disclosure, corruption, modification, and destruction. It generally acts as the first line of defense to avoid the unauthorized access and entry. It comprises a set of controls that restrict access to resources based on the group membership, identity, clearance, physical & logical location and need-to-know. In addition, the access can be in the method of permission to consume, enter, control, restrict, use and protect the resource to guarantee three basic principles such as availability, Confidentiality, and Integrity.

Source:
https://www.hack2secure.com/blogs/an-introduction-to-core-security-concepts-cia-triad-and-aaa