**Classification Guide - Security Objectives**

**Security Objectives:**

Project documentation often contains security-relevant statements that are indicative of the security requirements of a system. To identify security-relevant statements in project documentation, it can be helpful to think in terms of security objectives of the software system. The following table provides a guide for understanding security objectives and a guide to identifying statements that indicate the need for each security objective.

|  |  |
| --- | --- |
| **Confidentiality (C)** | The degree to which the "data is disclosed only as intended" |
|  | Statements that indicate a need for confidentiality:   * presence of read-type verbs (read, view, display, share, alert, use, export, retrieve, report etc) when accessing a sensitive resource * securing or restricting access to a sensitive resource * specification of user roles and access rules (e.g., granting or revoking access) |
| **Integrity (I)** | "The degree to which a system or component prevents unauthorized access to, or modification of, computer programs or data." |
|  | Statements that indicate a need for integrity:   * presence of write-type verbs (create, update, delete, save, auto-populate, review, verify, generate, define, apply etc) when accessing a sensitive resource * accuracy, consistent understanding and interpretation of sensitive information * auto-population or merging of sensitive information * environmental checks (firewall, denial of service, virus checking, app firewalls) |
| **Identification & Authentication (IA)** | The need to establish that "a claimed identity is valid" for a user, process or device. |
|  | Statements that indicate a need for identification & authentication:   * need to identify / verify the entity (user or system) accessing a sensitive resource * need to identify / verify the source of data (e.g., patient originated data vs. clinic originated data) |
| **Availability (A)** | "The degree to which a system or component is operational and accessible when required for use." |
|  | Statements that indicate a need for availability:   * time or location constraints on information (e.g., real-time information) * data retention, historical or longitudinal data (available over a period of time) * checks and limits on resource utilization * backups, replication or archiving of resources |
| **Accountability (AY)** | Degree to which actions affecting software assets "can be traced to the actor responsible for the action" |
|  | Statements that indicate a need for accountability:   * recording of actions (e.g., accessing a resource) related to sensitive resources * recording of events (e.g., alerts and notifications) related to sensitive resources * ability to reconstruct history of actions and events * preventing someone or a component from denying they performed an action * transactions of data (create, read, update, delete, merge, unmerge, assign, …) |
| **Privacy (PR)** | The degree to which an actor can understand and control how their information is used. |
|  | Statements that indicate a need for privacy:   * ability of an individual to exercise control over the collection, use and dissemination of his or her personally identifiable information (e.g., by providing consent) * gathering, usage, disclosure, and management of user or client data * masking of the identity of specific users or individuals * legal and compliance issues related to personally identifiable information |