Saltzer's and Schroeder's Design Principles

Principle of Economy of Mechanism. The protection mechanism should have a simple and small design.

Principle of Fail-safe Defaults. The protection mechanism should deny access by default, and grant access only when explicit permission exists.

Principle of Complete Mediation. The protection mechanism should check every access to every object.

Principle of Open Design. The protection mechanism should not depend on attackers being ignorant of its design to succeed. It may however be based on the attacker's ignorance of specific information such as passwords or cipher keys.

Principle of Separation of Privilege. The protection mechanism should grant access based on more than one piece of information.

Principle of Least Privilege. The protection mechanism should force every process to operate with the minimum privileges needed to perform its task.

Principle of Least Common Mechanism. The protection mechanism should be shared as little as possible among users.

Principle of Psychological Acceptability. The protection mechanism should be easy to use (at least as easy as not using it).