Principles -

Kerckhoffs's principle

Only keep hidden the key.
(e.g., make the construction, and constants public)

Principle of (key) separation

Use different keys for different contexts, compartmentalize.
(e.g., minimise the damage of a leak)

Principle of diversity

Use different types of … cryptographic algorithms.
(e.g., avoid same attacks against all)

Principle of simplicity

Keep everything simple.
(e.g., unnecessary complexity brings in risks)

Security by default

Keep default configuration as secure as possible.
(e.g., deny access by default)

Ethics!

Principle of minimal trust

Minimise the number of trusted entities, don't trust easily.
(e.g., do not say your secret to everyone)

Principle of the weakest link

A system cannot be more secure than its weaker component (link).
(e.g., secure all components)

Principle of least privilege

Grant the exact privileges required to perform the job.
(e.g., do not grand less or more privileges)

Security by design

Build in security from start.
(e.g., integrate security in the design and all the phases of the system)

Principle of modularization

Keep things modular.
(e.g., easily change one cipher with another)

Defence in depth

Use diverse security strategies at different layers.
(e.g., use physical and technical security)

Security by obscurity (?)

Oblivious Transfer, Obfuscation, Covert Channels, … , Kleptography, Standardisation …