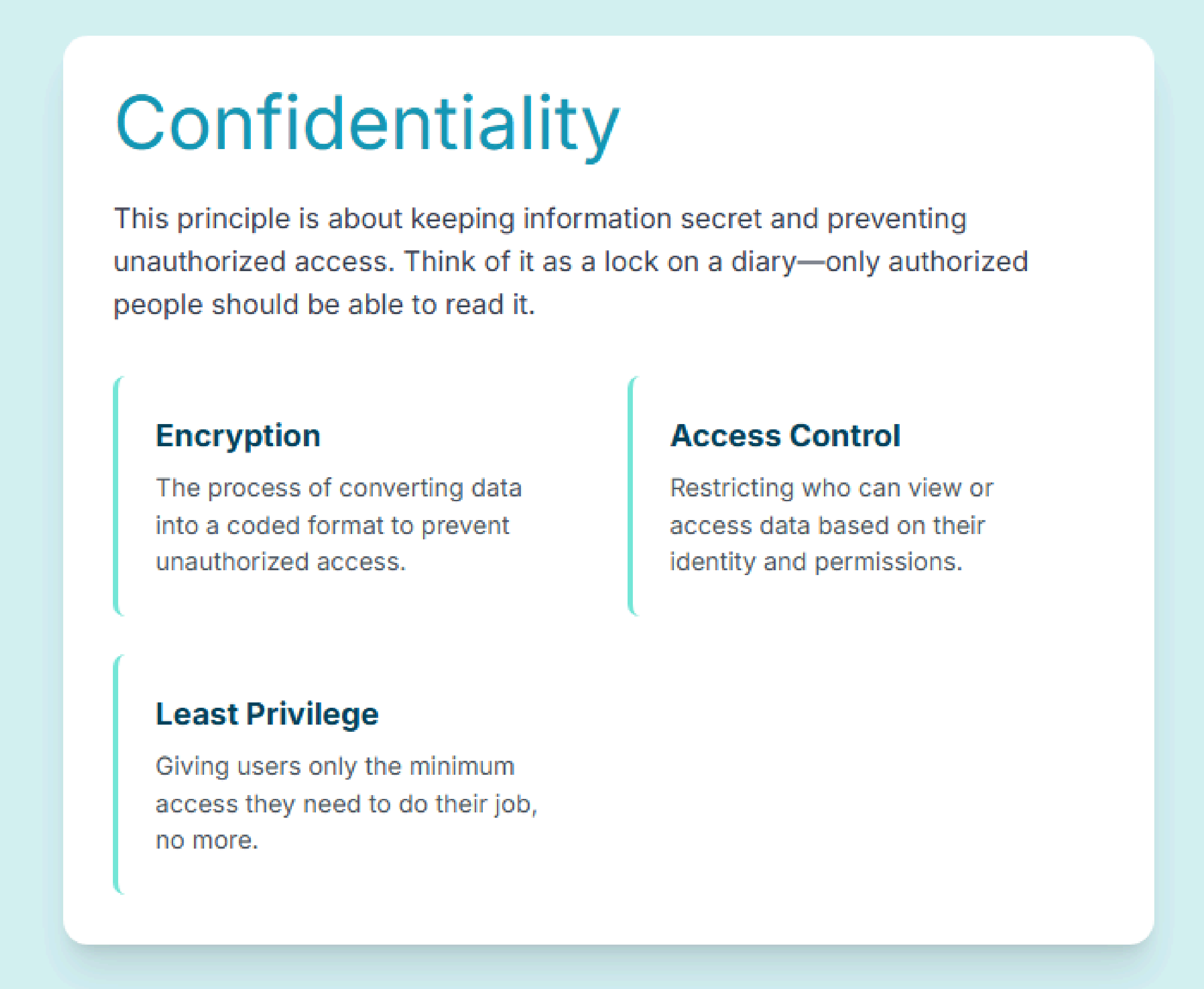
The CIA Triad

The foundational model for information security, representing the three core principles that must be upheld to protect data in any system.

An Interactive Overview

The principles of Confidentiality, Integrity, and Availability are interconnected and equally crucial for a robust security posture. Click on a segment of the donut chart below to navigate directly to that principle's section.

Confidentiality
Integrity
Availability



Confidentiality

This principle is about keeping information secret and preventing unauthorized access. Think of it as a lock on a diary—only authorized people should be able to read it.

Encryption

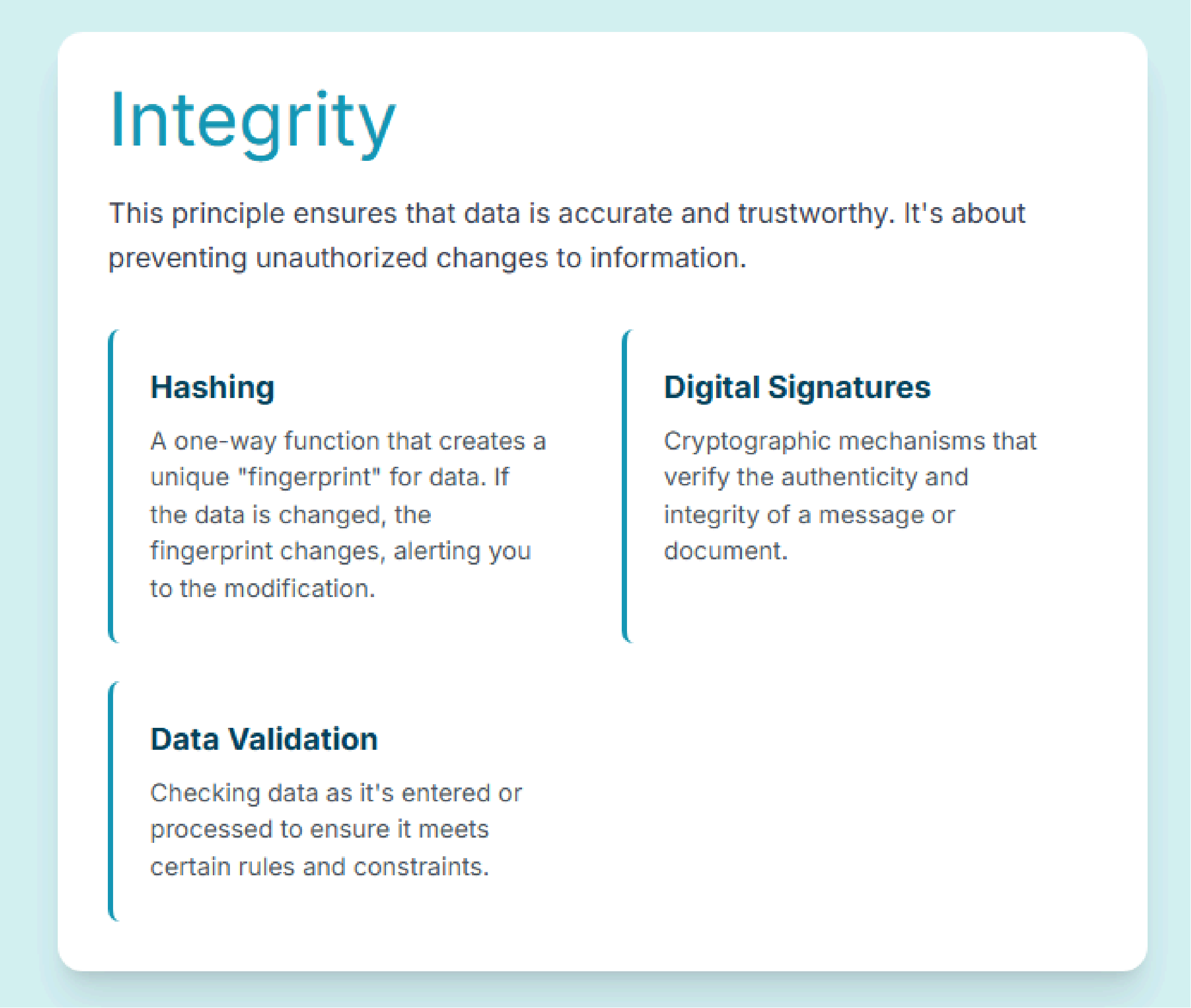
The process of converting data into a coded format to prevent unauthorized access.

Access Control

Restricting who can view or access data based on their identity and permissions.

Least Privilege

Giving users only the minimum access they need to do their job, no more.



Integrity

This principle ensures that data is accurate and trustworthy. It's about preventing unauthorized changes to information.

Hashing

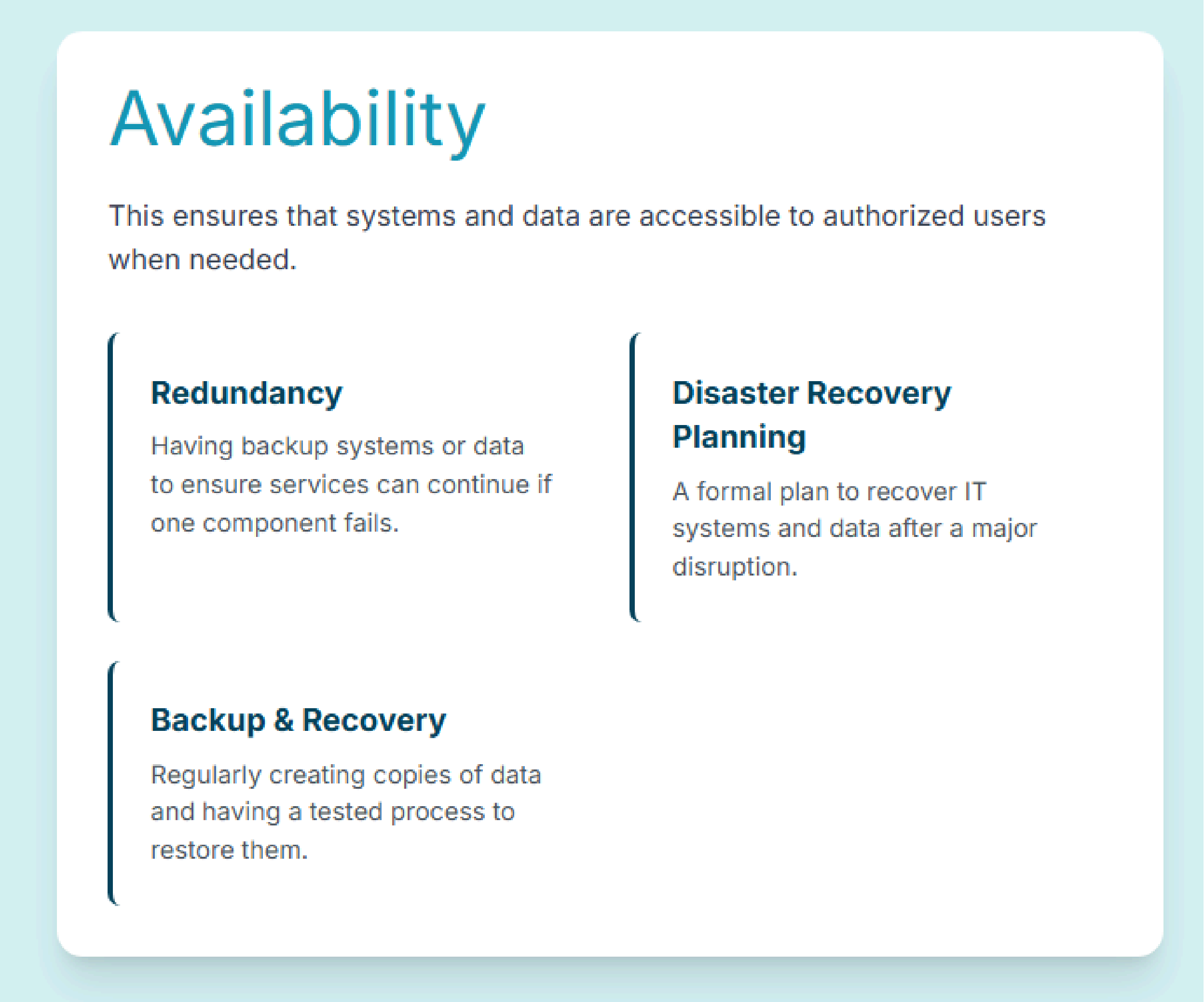
A one-way function that creates a unique "fingerprint" for data. If the data is changed, the fingerprint changes, alerting you to the modification.

Digital Signatures

Cryptographic mechanisms that verify the authenticity and integrity of a message or document.

Data Validation

Checking data as it's entered or processed to ensure it meets certain rules and constraints.



Availability

This ensures that systems and data are accessible to authorized users when needed.

Redundancy

Having backup systems or data to ensure services can continue if one component fails.

Disaster Recovery Planning

A formal plan to recover IT systems and data after a major disruption.

Backup & Recovery

Regularly creating copies of data and having a tested process to restore them.