Presidio Principles

Foundational Values for a Decentralized Future

Preamble

Blockchain technology, a pillar of the Fourth Industrial Revolution, can not only unlock radical improvements across the public and private sectors, but also enable new business and governance models that help enhance security, accountability, and transparency for people worldwide. However, innovation that progresses without sufficient consideration for governance and user protection often leads to undesirable outcomes for individuals, companies and organizations, and society at large.

The World Economic Forum's Global Blockchain Council drafted the following principles to help safeguard the promise of this technology. We hope that this document will provide creators of blockchain applications with a baseline for designing systems that preserve the rights of their participants.

We call on all actors, including developers, governments, executives, international organizations, corporate boards, and others, to uphold these tenets as they build blockchain applications – and to self-direct their ecosystems in using these principles as a foundational vision for how users can and should be protected.

We encourage participants and policymakers to leverage these principles as they seek to bring greater accountability to the systems that power our societies.

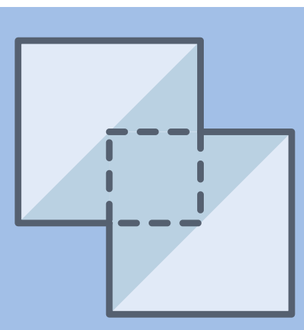
These principles are intended to serve as a steering document for the community. This document is not legally binding and is intended to be aspirational.

Presidio Principles

Foundational Values for a Decentralized Future

Applications built on top of blockchain-based systems should preserve the following participant rights.

Transparency & Accessibility

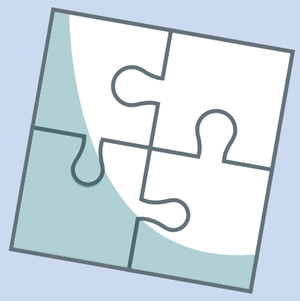


The right to information about the system.

A participant should have access to information that would enable them to:

1. Understand how a service is operated, including potential risks of the service, availability of source code, and the rules and standards upon which it is based.
2. Understand the potential risks and benefits of a service's use of blockchain technology.
3. Understand system performance expectations and where the responsibility for service delivery lies.
4. Understand the rights and obligations of different participants in the system.

Agency & Interoperability



The right for participants to own and manage their data.

A participant should be able to:

5. Create, manage, and independently store cryptographic keys.
6. Manage consent of data stored in third-party systems.
7. Port data between interoperable systems or parts of a system.
8. Revoke consent for future data collection system.
9. Have access to information sufficient to facilitate system interoperability.

Privacy & Security

The right to data protection.

A participant should be able to:

10. Assess if their data is at risk through appropriate disclosure procedures, which may include, but are not limited to, an examination of audit results, certifications, or source code.
11. Have their data protected in accordance with internationally recognized technical security standards.
12. Limit data collection to that which is necessary and data use to the purpose for which it was provided.
13. Verify – through third-party or self-created tools – that operations have been completed and confirmed in accordance with the system's rules.

Accountability & Governance

The right for participants to understand available recourse.

A participant should be able to:

14. Access information needed to: (a) understand the system's governance and rules and (b) pursue effective recourse mechanisms.
15. Opt-out of using applications that don't treat data in accordance with internationally recognized governance and data protection standards.
16. Rectify demonstrably false, inaccurate, or incomplete data when necessary.