COMPANY LOGO

SOC 2 Compliance

Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles": **security, availability, processing integrity, confidentiality and privacy.**

Why SOC 2 Compliance is Important?

1. Improved information security practices – better defend itself better against cyber attacks and prevent breaches.

2. A competitive advantage – because customers prefer to work with service providers that can prove they have solid information security practices, especially for IT and cloud services.

Why SOC 2 Compliance is Important?

1. Improved information security practices – via SOC 2 guidelines, the organization can better defend itself better against cyber attacks and prevent breaches.

2. A competitive advantage – because customers prefer to work with service providers that can prove they have solid information security practices, especially for IT and cloud services.

SOC 2 Checklist

Access controls—logical and physical restrictions on assets to prevent access by unauthorized personnel

Change management—a controlled process for managing changes to IT systems, and methods for preventing unauthorized changes.

System operations—controls that can monitor ongoing operations, detect and resolve any deviations from organizational procedures.

Mitigating risk—methods and activities that allow the organization to identify risks, as well as respond and mitigate them, while addressing any subsequent business.

Contact Us: 1-800-123-1234

hello@companydomain.com