How Rewind Backups Enables SOC 2 Compliance

rewind

The goal of SOC 2 (an acronym for "service organization control") is to create a set of guidelines that will lead to applications built with privacy, security, availability, integrity, and confidentiality in mind.

Below is a checklist that shows how Rewind Backups for GitHub can help regarding each SOC 2 criteria.

1. Security Criteria (Mandatory for SOC 2)

According to the AICPA (the organization that designs the SOC 2 Trust Services Criteria and regulates SOC auditors), "*Security*" refers to "*Information during its collection or creation, use, processing, transmission, and storage*". It also includes all systems that use electronic information to "*enable the entity* (e.g. your business) *to meet its objectives.*"

This means that your internal processes as well as other third-party applications, tools, or SaaS products should also comply with SOC 2 security requirements. This is a confident demonstration that your customer data is handled securely throughout your supply chain.

How can Rewind help your company satisfy this criteria?

✓	**AES Encryption:** AES 256 bit encryption for your backups (in transit and at rest). Learn more →
✓	**Verified by GitHub:** Your GitHub credentials are used to sign in to Rewind Backups for GitHub. Learn more →
✓	**SOC 2 Report:** Rewind is SOC 2 compliant. Type 1 report is available to Rewind enterprise plan customers with NDA. Learn more →

2. Availability Criteria

The availability trust service principle means that your systems must be ready and able to run as expected based on your operating agreements with customers and/or users.

Availability criteria often involve documented business continuity and disaster recovery plans and procedures. Potential customers will want to know what your plan is in the event of an emergency. The availability criteria also require periodic backups and recovery tests of business-critical applications

How can Rewind help your company satisfy this criteria?

✓	**Automated Daily Backups:** You will have automatic daily backups to secure your critical data on GitHub.
✓	**Rapid, Self-Serve Restores:** You can restore your repositories in a few clicks through the self-serve portal in a few clicks.
✓	**Restore Tests:** Restore tests, often required for compliance, can be conducted in minutes with Rewind's self-serve portal.
✓	**Metadata Backups:** Your GitHub metadata is included in backups and restores (pull requests, issues, milestones, etc). Here's a full list of what Rewind for GitHub backs up.
✓	**Cloud Sync:** You can have an automatic copy of your backups on your Amazon S3 or Azure Blob storage. This feature is available with Enterprise plans. Learn more →
✓	**Clone from Rewind Servers:** If GitHub servers are down, you can clone your GitHub data from Rewind servers. Learn more →

3. Confidentiality Criteria

This criterion requires that information designated as confidential is protected. The level of protection will depend on the type of information and industry: for example, data related to health care falls under more stringent regulations known as HIPAA.

How can Rewind help your company satisfy this criteria?

✓	**GDPR Compliant:** Rewind is GDPR compliant. Learn more →
✓	**Advanced Audit Log:** Rewind Backups provides a detailed audit log, which is a centralized stream of all system and user activity within your Rewind account. This feature is available with Enterprise plans. Learn more →

4. Processing Integrity Criteria

Industries where the accuracy of information processed is vital, such as services that perform financial transactions or data analytics for their customers, often consider covering processing integrity criteria in their SOC 2 report. Basically, this criteria asks the question: how do you ensure that the information you are processing is complete, valid, accurate, timely, and authorized?

✓	**Cloud Storage of Choice:** You can choose your backup storage location (US or EU) for your GitHub data storage to comply with regulations such as GDPR.

5. Privacy Criteria

Privacy criteria aims to ensure that "*personal information is used, collected, retained and disclosed to meet the entity's objectives*." While confidentiality applies to various types of sensitive information, such as financial data or health records, privacy applies only to the personal information you have collected about or on behalf of customers and/or clients.

✓	**Read Only Access:** Rewind only requires read-only access to your data for backups.
✓	**Repository Selection:** You can select which repositories you'd like to backup or select all repositories depending on your needs or privacy concerns.
✓	**Write Access for Restores Only:** Rewind only gets write access to your data through a separate app when you need to restore your data. Learn more →

Protect your data with Rewind Backups for GitHub today.

START FREE TRIAL

rewind