narratize

Proprietary Data FAQ

At Narratize, we understand the importance and sensitivity of your proprietary data. Protecting your insights and intellectual property is our highest priority. Below, we've proactively addressed common security questions to reassure you that your data is safe and secure with Narratize.

How does Narratize protect my proprietary data?

We utilize robust security measures, including advanced encryption (AES-256) for data both at rest and in transit (TLS 1.2+), strict access controls with multi-factor authentication, and ongoing vulnerability assessments and penetration tests.

Is my data encrypted?

Yes. All data transmitted and stored by Narratize is protected using industry-leading encryption protocols. Data-at-rest is encrypted using AES-256, and data-in-transit employs TLS 1.2 or higher.

Who has access to my data?

Narratize strictly adheres to the principle of least privilege, granting team members access only to the specific data required for their roles. Administrative access is highly restricted, regularly audited, and requires multi-factor authentication.

What security compliance standards does Narratize follow?

Narratize adheres to AICPA Trust Services Principles and conducts annual external audits, as well as continuous vulnerability scans and both internal and external penetration tests. Our security policies and practices are regularly reviewed and updated to maintain compliance with the latest regulatory and industry standards.

Where is my data stored?

Narratize stores data securely with leading third-party cloud providers, such as AWS, with rigorous backup, redundancy, and recovery protocols in place. These providers comply with extensive security certifications and regulatory standards.

How long does Narratize retain my data?

Data retention aligns with your active account status and contractual agreements. Upon request or termination, data is securely disposed of within 30 days, unless legally required otherwise.

How does Narratize handle third-party vendor security?

We conduct thorough security assessments before partnering with third-party providers and continuously monitor their compliance through independent audits and penetration tests.

Does Narratize have a disaster recovery plan?

Absolutely. Narratize maintains a comprehensive Business Continuity and Disaster Recovery Plan. Daily backups are automated, and recovery procedures are regularly tested and validated.

What responsibilities do I have regarding data security?

While Narratize provides extensive security measures, we encourage best practices such as creating strong passwords, managing user access responsibly, and carefully assessing the sensitivity of the data you input into our systems.

Does Narratize use my data to train their models?

No. Your data is never used for training ML models external to your individual access.

What if I discover a vulnerability?

Please immediately contact us at **admin@narratize.com**. We actively encourage responsible disclosure and promptly address all security concerns.

Safeguarding your proprietary data is foundational to our partnership. We continuously invest in our security infrastructure so you can confidently innovate, collaborate, and grow.