Barrow

November 20, 2026

DATA SECURITY

How Barrow protects your firm's data

What to know about how Barrow handles your firm's documents and reports.

Kept to your firm

Every project, source document and report belongs to one firm and is available only to that firm's members.

Never used for training

Your data is never used to train or improve AI models. Each firm's data is processed in isolation, with no exposure to other customers.

Used only for your work

Your documents and report content are processed only to provide the research, drafting and review features you request.

Yours

Everything you upload and the reports you produce remain yours. We do not sell customer information.

Encrypted, and stored in the United States

Data is encrypted in transit with TLS 1.2 or higher. Customer files are encrypted at rest with AES-256. Customer files are stored in Amazon S3 in United States regions, and the Barrow service runs in the United States.

Your firm's own sign-in

A firm can have its people sign in to Barrow, on the web and in Barrow for Word, with their company Microsoft accounts. Barrow does not receive or store passwords.

Barrow maintains a written Information Security Policy covering access control, data classification and handling, encryption, AI data use, incident response, backup, monitoring and vendor management. It is reviewed annually and is available to customers on request.

For your IT team: barrow.site/security **On the web:** barrow.site/data-security **Questions:** support@barrow.site