articulate

Articulate 360 Security Policy

This policy was updated in October 2026.

Articulate 360 is a learning intelligence platform that helps organizations turn what they know into what their people can do. It combines modern creation formats, AI grounded in learning science, and enterprise-grade admin and security controls, so learning and development (L&D) and other teams across the business can create training that builds real capability and scale it consistently.

You may have questions about how we keep your data safe as you use this platform. This policy outlines how we protect your information through our security infrastructure, rigorous internal practices, and strategic partnerships with vendors like Amazon.

How Articulate 360 Works

The Articulate 360 platform offers two primary products: Articulate 360 AI and Frontline. Frontline is a web-only product, while Articulate 360 AI has both web and desktop tools. Web products and tools run in a web browser. Desktop apps run locally on a computer.

The following tables provide an overview of the products and tools available in Articulate 360:

Articulate 360 Products

Product name	Product type	What you can do with the product
Frontline	Web	Turn product updates, process changes, and policy shifts into structured training that builds real capability, with L&D's standards built in.
Articulate 360 AI	Web and Desktop	Create and deliver training that changes behavior, scale it across the organization, and prove it's working. See the Articulate 360 AI Tools table below for the tools included with Articulate 360 AI.

Articulate 360 AI Tools		
Tool name	**Tool type**	**What you can do with the tool**
Storyline	Desktop	Create immersive, highly customized learning experiences to fit the needs of any training situation.
Rise	Web	Create high-quality training with guided, form-based authoring that incorporates learning best practices.
Review	Web	Streamline the feedback process and collaborate with stakeholders to speed up training development.
Reach	Web	Launch training, manage users, and measure success with a frictionless LMS built to distribute content quickly and easily.
Localization	Web	Develop, localize, and validate courses within the Articulate authoring platform to upskill global learners faster and more effectively.

Note: Articulate 360 AI currently provides access to the following desktop apps: Studio 360 (which includes Presenter 360, Quizmaker 360, and Engage 360), Replay 360, and Peek 360. Updates and technical support for these apps will end on December 31, 2026.

Articulate 360 desktop tools, like Storyline, save your data locally on your computer. They don't require a persistent internet connection and can run offline for up to 99 days at a time. If you have an internet connection, desktop apps will occasionally connect to the Articulate infrastructure hosted by Amazon Web Services (AWS) to access assets and collect data to improve our products and services. Learn more about Articulate 360 network endpoints.

When you install a desktop app on a device administered by your IT department, any work you do is protected by your company's security policies.

Articulate 360 web products, such as Frontline, and web tools, such as Rise and Review, work exclusively in the cloud. Keep reading to learn how we keep your data safe on our web-based products and tools.

Addressing Common Security Concerns

When companies vet cloud-based solutions, three core concerns arise: data theft, data loss, and downtime. We designed our security infrastructure to protect your information from these potential threats. Learn more about our processes for hosting and disaster recovery, encryption and data protection, data management, data privacy, and artificial intelligence below.

Hosting and Disaster Recovery

Articulate uses Amazon Web Services (AWS) as its hosting provider, with a U.S. data center in northern Virginia and an EU data center in Germany. Articulate 360 services are redundant across at least three isolated and resource-independent availability zones. This redundancy ensures that up to two data centers can go offline simultaneously while we continue to provide customers with a great experience. You can learn more about our services' uptime by visiting: https://www.articulatestatus.com.

Since Articulate's infrastructure exists as a virtual environment, it is entirely scalable. We perform capacity monitoring to ensure that resource usage (including available storage) stays within acceptable limits. We can also leverage Amazon Web Services (AWS) to accommodate additional capacity needs. Visit our Trust Center for a copy of our architectural diagram.

The Platform Engineering team performs frequent, fully automated customer data backups with up-to-the-minute recovery options. They also conduct nightly data recovery testing with full automation and monitoring to identify any issues during backup production or test restoration. This reduces the likelihood of data loss and minimizes downtime during large-scale disasters. Backup data is isolated from production systems and redundantly stored across multiple Availability Zones in AWS us-east-1 (Northern Virginia) or eu-central-1 (Frankfurt), depending on where the customer's subscription resides.

Encryption and Data Protection

Articulate uses the Amazon Web Services (AWS) Key Management Service (KMS) to manage the life cycle of keys within our AWS environment. KMS is natively supported by AWS services and backed by hardware security modules (HSMs).

Access to the KMS management console is restricted to approved Articulate personnel with role-based business needs only.

Articulate uses the latest encryption technology to secure all customer data. Articulate supports customer data encryption Transport Layer Security protocols 1.2 and 1.3 encryption methods for data in transit. Data at rest on our servers is encrypted using industry-standard algorithms such as AES 256.

Data Management

Articulate engineers have limited access to customer content to troubleshoot production outages. A small subset of our engineering team has full access to production infrastructure with safeguards in place, including two-factor authentication and short-leased, revocable sessions.

Our engineers use individual user accounts with two-factor authentication. A secure channel (VPN) and username/password authentication are required for any remote access to Articulate information and systems. All access to our AWS infrastructure is logged for auditing purposes. These practices are audited annually as part of our SOC 2 Type 2 Audit.

Data Privacy / General Data Protection Regulation (GDPR)

At Articulate, we value our worldwide customer base and your right to privacy.

Under the GDPR, if you are an employee or one of our customers' users, we are generally considered a data processor because we collect data when delivering e-learning services to our customers, who are considered data controllers. We engage carefully vetted subprocessors for specific purposes to provide e-learning services.

We require that each subprocessor agree to a Data Processing Agreement (DPA) that reflects our commitment to take data privacy obligations seriously.

Providing you with control over how we collect, retain, and use your data is a vital component of the GDPR. For more information about how Articulate aligns with the GDPR, please visit the GDPR section of our Trust Center.

Artificial Intelligence

Articulate 360 includes features powered by artificial intelligence (AI). Designed to help you create and deliver training more efficiently, these features are governed by our AI Responsible Use Policy and operate within our ISO 42001-certified AI management system, the international standard for the responsible governance of AI.

Customer content processed by our AI features is not used to train any generative AI models unless expressly authorized by you. AI processing follows the same encryption, access control, and regional hosting standards described above, and all subprocessors supporting these features are subject to the same Data Processing Agreement requirements as our other subprocessors.

Account owners or administrators can control whether AI features on Articulate 360 AI Teams subscription are available to users in their organization and can change that setting at any time. For help managing these settings, please check out this article.

For detailed information about our AI architecture, security controls, and data handling practices, please visit the Articulate Trust Center, where you'll find our AI Technical Architecture, AI Security and Privacy Whitepaper, and AI Detailed Security FAQ.

Internal Security Practices

Safeguarding customer data is an ongoing commitment. The following practices are in place to ensure we stay ahead of potential security threats.

We hire trustworthy people.

Articulate hires top engineers with proven industry track records to maintain our infrastructure. In addition, we provide ongoing internal and external training opportunities. Security engineers get content and training on security-specific processes and knowledge relevant to our security program.

We work with industry-leading partners.

We supplement our infrastructure with the technology and expertise of carefully vetted partners.

We take time to educate ourselves.

We provide continuous training to employees with access to customer data to help them understand the latest security threats and how to protect against them.

We use industry-leading testers to probe for potential vulnerabilities.

We regularly work with third-party penetration testing partners to identify potential vulnerabilities, enabling us to strengthen our security position. These vendors are trusted by many other high-tech clients, including Google and Microsoft.

We update our infrastructure continuously.

We perform weekly, monthly, and as-needed infrastructure maintenance to close vulnerabilities discovered by security researchers.

Summary

We work hard to maintain your trust so you can be confident about the safety of your data as you use Articulate products and tools. We've built a robust security infrastructure and hired skilled engineers to protect your information. And we're committed to protecting your data from theft, loss, downtime, and any other security threats.

Review the Articulate Trust Center for more information about our security practices. If you have any specific questions, please contact us at security@articulate.com.

articulate

Copyright ©2026 Articulate Global, LLC. All rights reserved.
Articulate and all other trademarks mentioned in this document are the property of their respective owners.