articulate

POLICY

Articulate 360 Security Policy

This policy was updated on July 24, 2023.

Articulate 360 is an annual subscription with everything you need to simplify the entire course development process. It includes our award-winning authoring apps, 10+ million course assets, a project review app, and live and on-demand online training with industry experts.

You may have questions about how we keep your data safe as you work with these apps and resources. This policy covers how we protect your information with our security infrastructure, rigorous internal practices, and strategic partnerships with vendors like Amazon.

How Articulate 360 Works

Articulate 360 includes desktop and web apps. Desktop apps run locally on your desktop or laptop computer, and web apps are software applications that run in a web browser.

Here's an overview of all the apps and resources included in Articulate 360:

App Type	App Name	What you can do in the App
Desktop App	Articulate 360 Desktop App	Install, launch, and update desktop-authoring apps; access web apps; and manage your account and profile
Desktop App	Storyline 360	Develop courses with custom interactivity that work on every device
Desktop App	Studio 360	Transform PowerPoint slides into e-learning
Desktop App	Replay 360	Walk learners through on-screen content by capturing screen activity and yourself on a webcam at the same time
Desktop App	Peek 360	Record screencasts on your Mac or Windows PC

App Type	App Name	What you can do in the App
Web App	Rise 360	Build fully responsive courses quickly
Web App	Review 360	Collect feedback from stakeholders and subject-matter experts on Storyline 360, Rise 360, Studio 360, Peek 360, and Replay 360 content
Web App	Content Library 360	Add 10+ million stock photos, templates, characters, videos, icons, and other images to your Articulate 360 courses
Web App	Reach 360	Distribute training directly to external and hard-to-reach learners—such as contractors, partners, franchises, and deskless workers—with this premium add-on to Articulate 360

Articulate 360 desktop apps save your data locally on your computer. They don't require an internet connection to run. If you have an internet connection, desktop apps will occasionally connect to the Articulate infrastructure hosted by Amazon Web Services (AWS) to access Content Library 360 assets, and collect data to improve our products and services. See this Knowledge Base article for more information.

Articulate 360 web apps, such as Rise 360 and Review 360, work exclusively in the cloud.

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. Since Articulate 360 web apps run on AWS servers, we know it's important for you to understand how we keep your data safe.

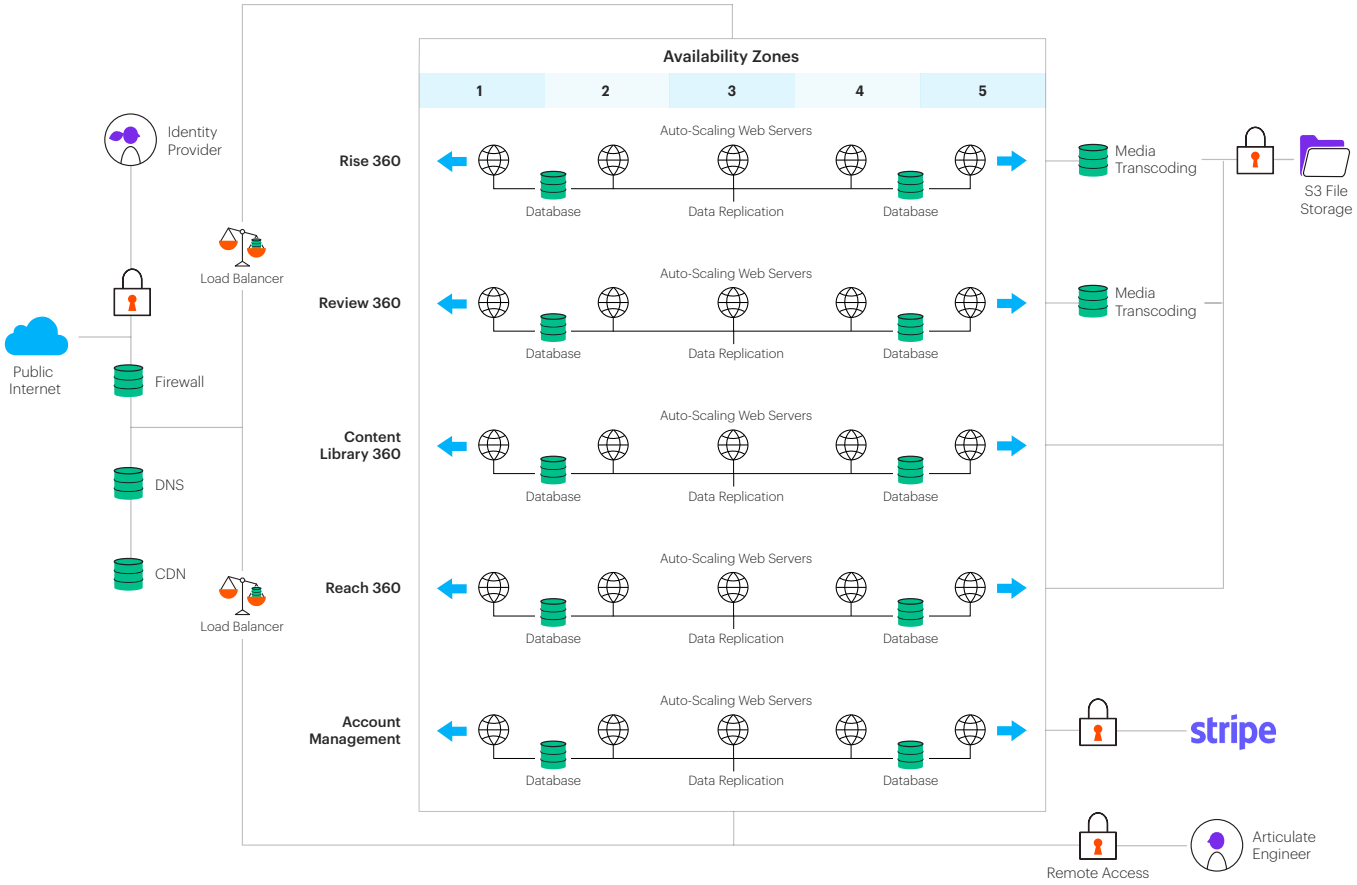
Addressing Common Security Concerns

Three core concerns come up when companies vet cloud-based solutions: data theft, data loss, and downtime. We designed our security infrastructure to protect your information from these potential threats.

Hosting and Disaster Recovery

Articulate uses Amazon Web Services (AWS) as its hosting provider. Articulate 360 services are redundant across five (5) 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.

Articulate's infrastructure exists as a virtual environment and is entirely scalable. Capacity monitoring is performed to ensure that the utilization of resources (including available storage) stays within acceptable limits. We also have the ability with Amazon Web Services (AWS) to accommodate any additional capacity needs quickly.



Our Systems Engineering team performs frequent, fully automated customer data backups and has implemented up-to-the-minute recovery options where feasible. We test our data recovery nightly with full automation and monitoring to alert us if there are any problems, either producing the backups or restoring them to a test location. This practice reduces the likelihood of data loss and minimizes downtime in a large-scale disaster.

Encryption and Data Protection

Articulate leverages 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 only approved Articulate personnel with role-based business needs.

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 standards (e.g., 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, each with a two-factor authentication requirement. A secure channel (VPN) and username/password authentication are required for all remote access to Articulate information and systems. All access to our AWS infrastructure is logged for auditing purposes.

These practices are annually audited 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, we are generally considered a data processor for the data we collect as we deliver e-learning services to our customers, the data controller. We engage carefully vetted sub-processors for specific purposes to provide e-learning services.

We require that each sub-processor sign and adhere to a Data Processing Agreement (DPA), which reflects our commitment, and that of our sub-processors, to take obligations with regard to data privacy 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.

Our Internal Security Practices

Safeguarding customer data is an ongoing commitment. We have several practices in place to make sure we stay ahead of potential security threats.

We hire trustworthy people.

Articulate hires top engineers with a proven track record in the industry to maintain our infrastructure. In addition, we provide ongoing internal and external training opportunities. Security engineers are provided content and trained 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. You'll find the full list of our vendors with links to their robust security policies in our Trust Center.

We take time to educate ourselves.

Employees with access to customer data receive continuous training 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 probe for potential vulnerabilities so that we can continue to strengthen our security position. These vendors are trusted by many 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 apps and resources. We've built our robust security infrastructure and hired skilled engineers to protect your information. And we're committed to protecting your data from data theft, data loss, downtime, and all 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