Articulate 360 Security White Paper

This white paper was updated on February 25, 2020

Articulate 360 is an annual subscription with everything you need to simplify the entire course development process. It includes our award-winning authoring apps, 5+ million course assets, a project review app, and live online training with industry experts.

You may have questions about how we keep your data safe as you work with these apps and resources. In this white paper, we'll cover 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 Apps	Articulate 360 Desktop App	Install, launch, and update desktop-authoring apps; access web apps; and manage your account and profile
	Storyline 360	Develop courses with custom interactivity that work on every device
	Studio 360	Transform PowerPoint slides into e-learning
	Replay 360	Walk learners through on-screen content by capturing screen activity and yourself on a webcam at the same time
	Peek 360	Record screencasts on your Mac or Windows PC
Web Apps	Rise 360	Build fully responsive courses quickly
	Review 360	Collect feedback from stakeholders and subject-matter experts on Storyline 360, Rise 360, Studio 360, Peek 360 , and Replay 360 content
	Content Library 360	Add 5+ million stock photos, templates, characters, videos, icons, and other images to your Articulate 360 courses

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.

Data Theft
You don't want unauthorized people to access your data.

We take several precautions to make sure no one can gain physical or remote access to your data on a server.

First, we partner with AWS to house your information in nondescript facilities located in Northern Virginia, USA. Trusted by clients such as the U.S. Department of State and Capital One, AWS has robust practices in place to keep their data centers secure. Read AWS's Overview of Security Processes for details.

Second, we use industry-standard encryption methods to protect your data as it moves into and out of AWS servers—such as when you're working in Rise 360 or publishing a course to Review 360. If an unauthorized person were to get ahold of your data while it was in transit or sitting at rest on our servers, they'd be unable to read it.

Finally, we employ the widely used authentication service OKTA to prevent anyone from remotely stealing your information and logging in to your Articulate 360 account.

Data Loss
You don't want to lose your data.

Data saved to the cloud is secure even if your computer is damaged, stolen, or destroyed. We make sure your data isn't lost to technical error or malicious deletion by automatically creating recoverable backup copies of your information as you work in Articulate 360 web apps.

Our engineering team takes extraordinary precautions to keep your data safe as they make updates to Articulate 360. Very few team members have the ability to delete customer data, and they work closely with each other in crews. No single employee is left alone with confidential and critical knowledge. All changes to our infrastructure are tracked and proactively monitored for suspicious activity.

Downtime
You don't want to lose access to your data.

Though technically not a security threat, downtime is a big inconvenience. We know you can't do your job effectively if the web tools you rely on go offline.

That's why we've chosen extremely reliable hosting and authentication vendors with track records of 99.5-99.9% uptime in a rolling monthly window. We also host your data across multiple AWS server storage facilities. That means more than one data center can be offline simultaneously and you still wouldn't lose access to Articulate 360 apps.

In the event of a disaster, we have a procedure in place to rebuild our entire data infrastructure and restore service as quickly as possible.

Note: Our status page notifies subscribers of security incidents and other issues.

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.
We hire senior engineers with strong track records and references so we can be confident that everyone on our team has the skills required to protect your data from the moment they join the team.

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 attend 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 our third-party penetration testing partner, Atredis, to probe for potential vulnerabilities so that we can continue to strengthen our security position. Atredis is 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 360 Trust Center for more information about our security practices. If you have any specific questions, please contact us at security@articulate.com.

articulate