Articulate Security Policy

This Policy was updated on June 2, 2022

At Articulate, we have developed robust engineering, security, and hiring processes to safeguard customer data. And we'd love to tell you a bit more about everything we do to keep your information secure.

Encryption

We apply the most advanced encryption technology publicly available to secure data. Using 256-bit TLS/SSL encryption and minimum 2048-bit RSA encryption, Articulate encrypts data at rest and network traffic, including on payment pages, into and out of Amazon Web Services (AWS).

Hiring Policy

We have a rigorous hiring process, requiring a full background check, to ensure that anyone we hire can perform their job function. We provide internal training when needed, but strive to hire experts with spectacular track records and references. Our employees work closely with each other in crews and teams, leaving no single employee alone with confidential and critical knowledge. Also, because we diligently interview and research referrals, we have yet to require background checks or drug testing.

Hosting

We host Articulate services in AWS servers in the us-east-1 region located in Northern Virginia in the United States. AWS data centers are state of the art, using innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and escorted continually by authorized staff.

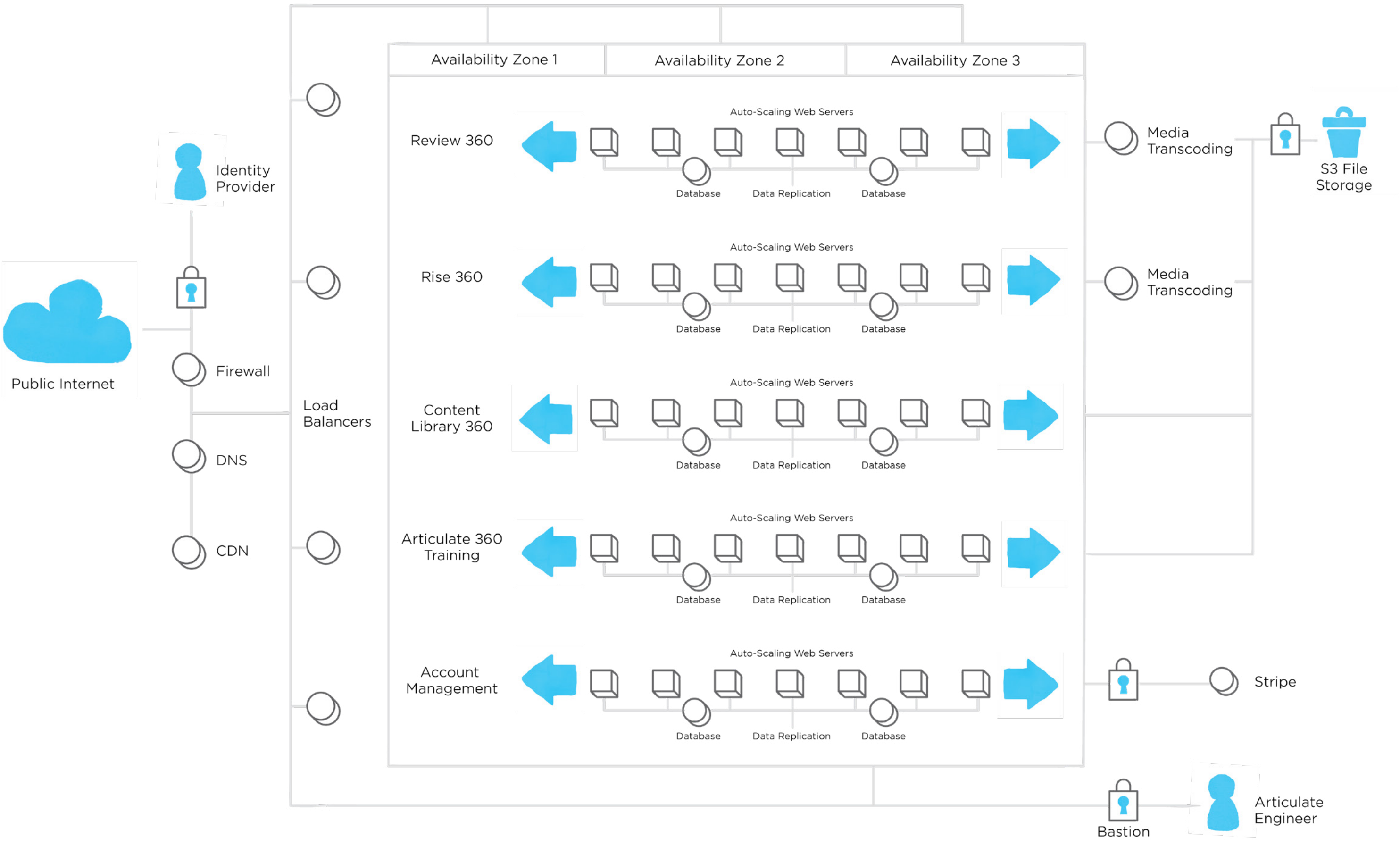
AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, access is revoked immediately, even if that person continues to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

AWS is trusted by over a million organizations, including security-focused companies such as FICO, Airbnb, Dow Jones, Intuit, and GE. If you'd like to learn more about AWS security practices, please check out these links:

- ISO Global Certification
- Overview of Security Processes
- Service Organization Controls Report
- AWS Customer Case Studies

We use many AWS-provided solutions including relational databases, full-text search, queuing, messaging, identity management, encryption, and caching. As part of our business continuity plans in case of disaster, we practice automated, routine, and frequent data backup and recovery. We aim to eliminate single points of failure in our infrastructure and have built redundancy into all our services. All Articulate services are redundant across three (3) or more physically isolated and resource-independent availability zones in Northern Virginia. That ensures multiple data centers can go offline simultaneously while we continue to provide customers with a great experience. Here's how our servers are structured within the AWS infrastructure:

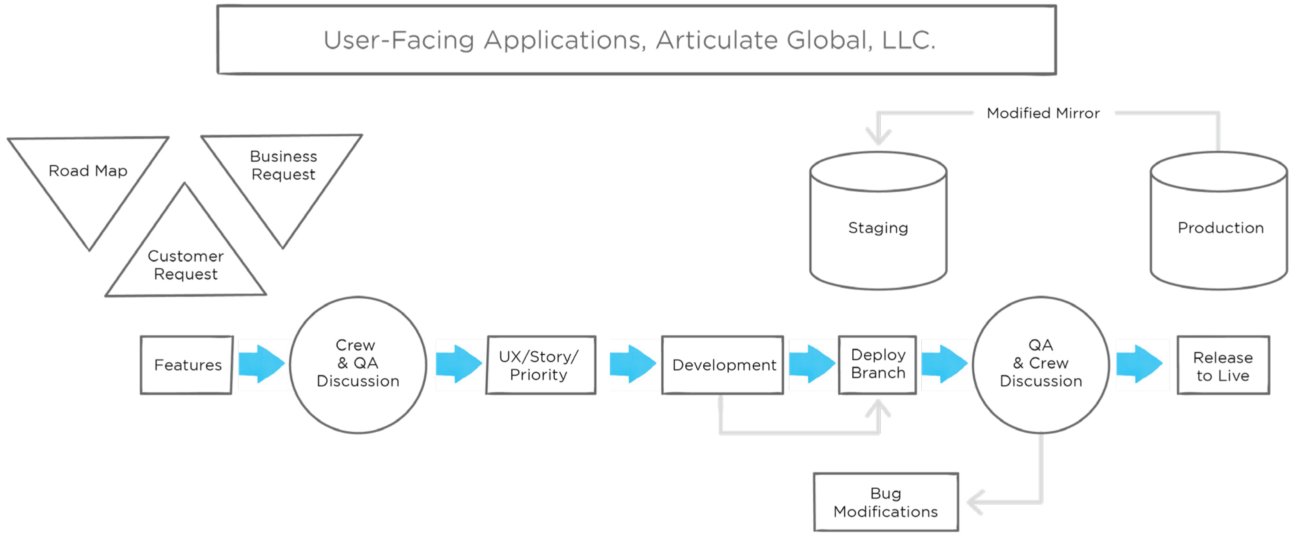


We use AWS CloudFront to efficiently serve content globally. CloudFront has numerous locations around the world, which lets us speed user access to content such as course assets (images, videos, audio), logos, characters, and course templates.

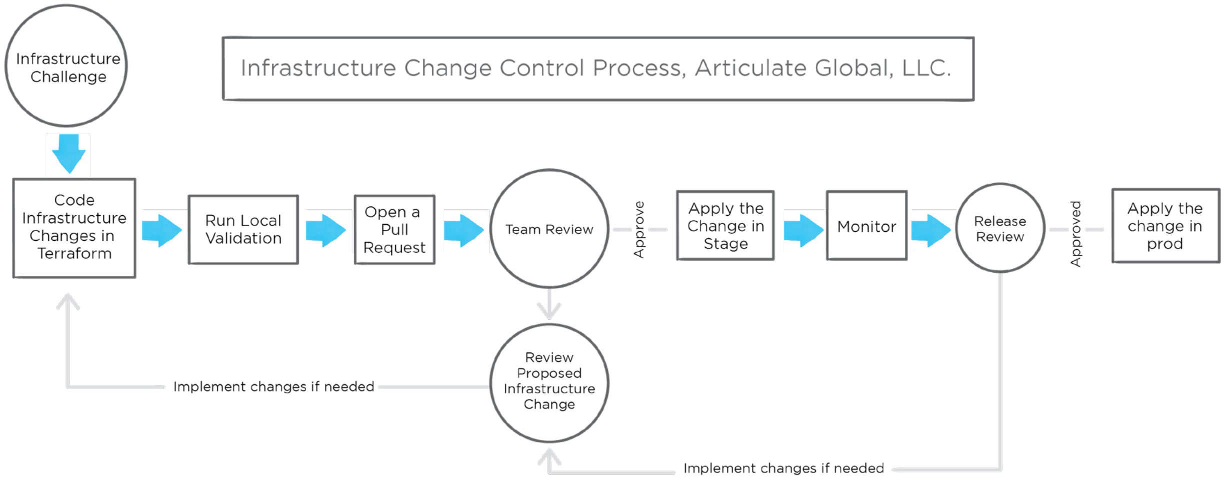
NOTE: To ensure access to essential Articulate services, be sure to whitelist the necessary endpoints, especially if connecting via a proxy.

Engineering and Quality Assurance (QA)

We develop all software in-house using GitHub as our code source repository. Our team develops software and conducts code reviews in local repositories using pull requests. Then, developers publish to our staging environment in protected branches for QA and business stakeholders to test. Here's an outline of our Software Development Life Cycle (SDLC) process:



We also have a formal process that outlines how our team updates our software and systems. Take a look:


Infrastructure Challenge
Infrastructure Change Control Process, Articulate Global, LLC.
Code Infrastructure Changes in Terraform
Run Local Validation
Open a Pull Request
Team Review
Approve
Apply the Change in Stage
Monitor
Release Review
Approved
Apply the change in prod
Review Proposed Infrastructure Change
Implement changes if needed
Implement changes if needed

User Authentication

We utilize best practices to authenticate users who log into our sites and services. When a user signs up for an Articulate ID, they either provide their email address, or a team admin sends an invite to the user's email address.

Articulate does not store user credentials. We rely on a third-party service, Okta, as our authentication provider. Okta implements proven, common, and popular identity protocols used in both consumer-oriented web products and enterprise identity infrastructures.

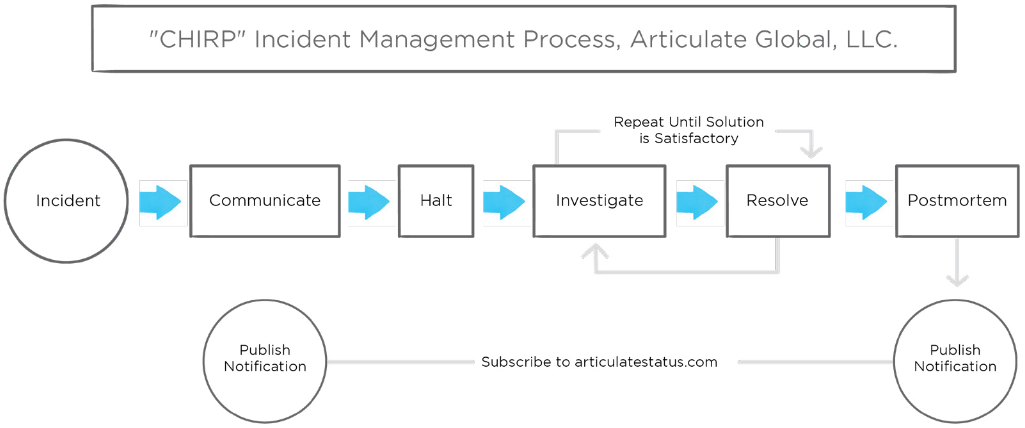
Articulate ID credentials are passed to Okta for authentication and Okta returns a JWT. The user creates an initial password and that process requires that the user has access to their email account.

The traffic between clients and the API gateway (Kong) and between the API gateway and Okta is all TLS 1.2 encrypted (industry standard). Okta uses AWS EBS encryption at rest (AES-256). When we use credentials supplied by Okta to authorize access to Articulate 360 APIs, the credentials are verified cryptographically in the API gateway layer before requests are passed along to the Articulate 360 APIs. In Okta, the passwords are hashed (and salted) securely using bcrypt.

For more details about Okta security processes, please check out the Okta Security Technical Whitepaper.

Disaster Recovery and Incident Management

Our team is prepared to respond to any emergency or interruption. We have a simple process we follow to make sure we communicate with anyone who's affected and do everything possible to prevent similar incidents from happening again. This diagram shows our response approach in more detail:


"CHIRP" Incident Management Process, Articulate Global, LLC.
Repeat Until Solution is Satisfactory
Incident
Communicate
Halt
Investigate
Resolve
Postmortem
Publish Notification
Subscribe to articulatestatus.com
Publish Notification

During any outages, we'll post updates to articulatestatus.com. Please subscribe to ensure you receive notifications.

Training

We recognize the importance of compliance training and partner with a leading vendor to conduct training for our team. Our goal is to increase security awareness and ensure that our customer-facing teams follow Payment Card Industry (PCI) compliance protocols.

Collaboration

Articulate products offer collaboration features and other integrated tools that allow you to share your content through Articulate software. As a function of the collaborative nature of Articulate software and based on the permissions and settings you choose, the use of such features enables the sharing of content with people you want to collaborate with or with the public. You can choose to change your settings at any time for a file or folder through your account. For more information about such collaboration and sharing features, we encourage you to review this article.