SECURITY

Robal Tech applications are built upon Amazon Web Services (AWS), the world's most comprehensive and broadly adopted cloud platform.

Security and Compliance is a shared responsibility between AWS and Robal.

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Services

Robal assumes responsibility and management of the operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS provided security group firewall using AWS WAF & Shield services. Robal manages its own AWS based cloud system.

Our AWS Console is only accessed by authorized IAM Users, remaining compliant with Multi Factor Authentication, as well as programmatic roles for our code solutions. Our users and roles are based on security policies, using only the access and responsibilities they need, providing security in our infrastructure and running services to allow only the correct personal needed to specific areas and privileges.

Our database is built in **DynamoDB.** All data stored in Amazon DynamoDB is fully encrypted at rest and we use AWS Beanstalk services to provide a server-less process to encrypt our payloads in transit between our web application and our API calls.

All of our assets are blocked for public access, and we use only CloudFront Origin Access Identity policies to allow only our internal infrastructure to use and consume our documents

and files, as well on our FrontEnd code we use signed URLs to be able to download, load and view on our Robal forms.

Amazon S3

Robal stores images and documents in Amazon S3. S3 encrypts all object uploads to all buckets. S3 is the only object storage service that allows you to block public access to all of your objects at the bucket or the account level with S3 Block Public Access.

S3 maintains compliance programs, such as PCI-DSS, HIPAA/HITECH, FedRAMP, EU Data Protection Directive, and FISMA, to help us meet regulatory requirements. AWS also supports numerous auditing capabilities to monitor access requests to our S3 resources.

AWS AppSync

We use **AWS AppSync** as our API to connect our application and services to data and events with secure, server-less and high-performing GraphQL queries.

AWS AppSync, like all AWS services, makes use of TLS1.2 and beyond for communication when using the AWS published APIs and SDKs. Using AWS AppSync, with other AWS services such as Amazon DynamoDB, ensures encryption in transit.

App Sync uses Cognito Authorization based on our user database, which assures a valid user that is authenticated is able to consume our API and we also establish a base role group and user identification for Authorization and ownership of data, this helps users only consume, modify and view data related to their role and group limits.

AWS CloudFront

Robal uses **AWS CloudFront** which is a Content Delivery Network that speeds up distribution of our static and dynamic web content, such as .html, .css, .js, and image files, to our users. CloudFront delivers our content through a worldwide network of data centers called edge locations.

When a user requests content that we are serving with CloudFront, the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possible performance. CloudFront is the only service authorize to consume and use Robal assets (documents, files, images) on our S3 buckets.

The CloudFront API endpoints only accept HTTPS traffic. This means that when you send and receive information using our CloudFront API, our data—including distribution configurations, cache policies and origin request policies, key groups and public keys, and function code in CloudFront Functions—is always encrypted in transit. In addition, all requests sent to the CloudFront API endpoints are signed with AWS credentials and logged in AWS CloudTrail.

Firewalls, Identity Platforms, and Auditing

Robal uses **AWS WAF, a web application firewall service,** to create a web access control list (web ACL) to restrict access to our content. Based on conditions that we specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront responds to requests either with the requested content or with an HTTP 403 status code (Forbidden).

Robal uses **AWS Cognito** as an identity platform for web and mobile apps. It's a user directory, an authentication server, and an authorization service for OAuth 2.0 access tokens and AWS credentials.

Robal uses **DataDog** services as an auditor to regularly test and verify the effectiveness of our security and compliance with CLOUD SECURITY MANAGEMENT, covering the following standards:

PCI - v3.2.1

SOC 2 - v2

CIS - AWS - v1.5.0

HIPAA - v1

NIST 800-171 - v2BETA

GDPR - v1

ISO/IEC 27001 - v2

Essential Cloud Security Controls - v1

AWS Trusted Advisor