Security at Gocious

We understand how important the security and privacy of your data is. We are committed to providing our customers with a highly secure and reliable environment for its cloud-based application. Our commitment to security is never ending and as technologies and best practices evolve in this space, we strive to make sure we adopt them to keep your information secure.

If you have a security concern, complaint, or question, please e-mail security@gocious.com.

Authorizing Access

Customer data is stored only in Production environment. We have clear separation between Production and Test environments.

In Production environment, Developers have access to logs for monitoring and supporting incidents.

We consider *identity* as the first step in the security Our systems use the following as our Identity providers:

- Azure AD Authentication
- Auth0

Azure AD authentication is used as centralize identity access management system. Everyone in our organization will have an account in Azure AD with MFA (Multi Factor Authentication).

We believe access management is critical for Azure resources, a Role Based Access Control (RBAC) policy is used to identify and manage the access control.

Auth0 – Auth0 is identity provider for our users and is used to store user credential information.

Auth0 is compliant with ISO 27001, ISO 27018, SOC 2 Type II, EU-US Privacy shield framework, HIPA BAA and Gold start and PCI DSS Certified.

For more information about Auth0 security refer to Auth0 Security

Data Encryption in Transit and Rest

For more information about privacy and compliance refer to Azure Privacy and Compliance

For new and archived audit reports for Azure, refer to Azure Audit Reports

Data is encrypted in transit using HTTPS TLS 1.2 network protocol.

Data in Azure cloud is encrypted at rest and follows industry best data encryption practices. Encryption and decryption are done using 256-bit AES encryption and is FIPS 140-2 compliant.

For more information how Azure uses data at rest refer to Azure Encryption at Rest

Our system uses Stripe – a SaaS based subscription platform to manage subscription and payment information. Stripe is PCI Service Provider Level 1 certified service.

Network Security

Firewall – Data ingress to our systems is controlled by Azure Web Application Firewall which is based on the rules from OWASP.

DDoS (Distribute Denial of Service) Mitigation and Protection – Our systems use Azure DDoS service to safeguard from DDoS attacks. An L-7 Load balancer, application gateway is used to mitigate DDoS attacks.

Incident Management

At Gocious, we have a thorough incident management process for security incidents and application errors.

An alert monitoring system will notify incidents to our triage team. The team will assess the impact and the priority for handling the incident. Based on the priority/severity of the incident, team will communicate and handle escalations.

The triage team will have the right tools and access to log monitors to troubleshoot and restore the service.

RCA (Root Cause Analysis) will be performed after every incident and will ensure that incident will not re-occur.

Monitoring

Our systems use Application Insights – Azure SaaS offering for monitoring availability, performance and usage of application. Alerts will be raised on anomaly behavior and our Incident management triage team will be notified.

Security Design

At Gocious, we believe in security first design.

Our systems use Continuous Integration and Continuous Deployment pipeline which have code review policy standards and release gates to all environments.

In addition to the CI/CD pipeline policy standards a periodic static code analysis is done using Veracode

Last updated: July 12, 2022