goosechase
Prepared for FAU

1. Product Information

- What is Goosechase?
- Proposal for FAU
- Types of Accounts
- How is data being processed?

2. Encryption

- General data encryption
- Backup encryption
- Crypto and key management scheme used
- Admin access

3. Server and Application Interface Security

- Data storage
- Protection of the production environment
- Application and supporting infrastructure design

4. Third Party

- Third party processors
- Transfer of data
- GDPR policy

5. Data Retention & Deletion

- Data retention
- Date deletion
- Backups
- Termination of the service agreement

6. Audit and Compliance

- Security vulnerabilities
- Privacy breaches
- Security Development

7. Change Control

- Logging activities & log safeguards
- Change control process

8. Human Resources

- Accountability for cyber security and security testing program
- Security team
- Team
- Team training
- Termination

9. Infrastructure and Virtualization Security

- Segregation of environments

10. Identity and Access Management

- Endpoint protection controls
- Restriction, log and monitoring access to our systems
- Ensuring that access to data is granted on as-needed basis
- Do you use multi-factor authentication for all privileged access?
- Preventing unauthorized access to systems, applications, users' data or source code
- Process for granting and documenting approval for access of tenant data

11. Incident Management

- Incident management process
- Monitoring infrastructure for identification of events related to specific users
- Enforcing and attesting to tenant data separation when producing data in response to legal subpoenas
- Contact in the unlikely event it would be needed

12. Integration

- Ways to safe-list the application
- Methods to integrate with other SaaS or on-premise systems
- RESTful APIs via an API Gateway
- Method of sending email notifications (to registrants & staff) from this system

Product Information

What is Goosechase?

At Goosechase, experience is everything. Originally inspired by scavenger hunts, Goosechase is an online platform that enables organizations and schools to engage, activate, and educate their communities through delightful interactive experiences.

Created online but played in the real world, Goosechase brings communities to life with engaging, interactive challenges designed to support organizations. The intuitive platform makes it easy to make a repeatable, fun, and positive impact on any community.

Since hatching in Canada in 2011, Goosechase has powered hundreds of thousands of global team building, training, fundraising, educational, tourist, and recreational experiences.

3 year Proposal for FAU

FAU shall have rights to the use of the GooseChase platform for unlimited experiences with unlimited participants, unlimited missions and mission types, Notifications and all new released features in the Goosechase platform for the duration of 3 years from the date of renewal.

Detailed Breakdown of License:

Full access to the GooseChase mobile apps and administrative web portal for Unlimited experiences for 3 years
Unlimited missions per game
All Current Goosechase features
First access to new GooseChase features
Dedicated CSM for Offsite Support, as necessary

Client Event Cost: $7,000/year (paid annually)

Goosechase in Education

Educators around the world use Goosechase as a way to reimagine lesson plans, create high learning impact opportunities and boost collaboration. The analytics and information generated through Goosechase from student participation allows educators to make changes based on the students behavior. Students and Educators alike are able to get hands on and see real time impact to their learning outcomes.

Product Information

Types of Accounts

Play as Guest;
The Play as a Guest option allows users to play without the need to create a Goosechase account. When participants select this option, they will be taken directly to the Join an Experience window and prompted to find their Experience by name or Join code in order to find and join an Experience as usual.

By playing as a Guest, their activity is only saved to their mobile device, and will not be saved to an online account. This activity will be deleted if they uninstall the Goosechase app from their device or reset the app from the settings menu.

For the avoidance of doubt, Goosechase will not collect any personally identifiable information through this option

Create an Account
Playing with an account allows a participant to tie all their activity to that account. Once an account is created, a participant can even sign in from another device to access all their data.
To sign up, a user will only need to create a username, chose their password, and add their email address. No other personally identifiable information will be requested to either create or maintain an account.

How is data being processed (i.e. who has access to customer data?)

Our platform ingests a range of mandatory and optional data.

For mandatory data, this is typically limited to IP addresses and the email address of the creator, as well as any additional information required for contact or billing purposes.

For optional data, this is highly dependent on how Experiences are set up and participants join. If Participants Play as Guest, data collected will be usage-based data whereas if they register for an account, it will be usage data and their email address.

Within the Experience, the type of data collected will be entirely contingent on the missions that are designed by the creator..

Encryption

How is data encrypted?

All customer data is encrypted during transit using TLS and SSL, with passwords salted and hashed. Given the lack of sensitive data that we collect, we currently do not encrypt data at rest. However, encryption at rest will be implemented in the second half of 2022 ahead of exciting new features.

How are admin systems accessed?

Accessing admin systems for our infrastructure requires 2FA, and accessing individual servers requires SSH key, password, and 2FA.

Backup encryption

Backups are encrypted in transit and at rest.

Crypto and key management scheme used

Passwords are salted and hashed.

Server and Application Interface Security

Data location, access and storage

Our platform is hosted on a combination of AWS and Linode infrastructure. Our staging environment is fully isolated and physically separated from our production environment and contains no customer data. As both servers are fully separate, hosted by two vastly different companies, the breach of one environment would not contaminate the other.

Ensuring that only tested and non-malicious code is released to production

Before any code is deployed, it needs to undergo a thorough code review by at least one other member of our team, along with complimentary automated testing. We use Automated unit testing, manual testing prior to release, segmented rollouts, exception and error tracking before any code is deployed

Application and supporting infrastructure design

Our backend infrastructure runs on virtualized Ubuntu servers powered by Linode. We use industry-standard practices for access control, in-flight encryption, and firewalling to ensure the security of our infrastructure and data. We also use full-disk backups to enable quick and effective recoveries in the case of data loss.

Third Party

List of other vendors or third party that may have access to tenant data or any subset of the data

Our full subprocessor list, along with the purpose of each, is available at: https://www.goosechase.com/sub-processors

Do we share data?

In general, we only ever share data with a third party for a specific purpose, such as improving our product through anonymized usage analytics. For anything related to advertising/marketing, we only share information upon explicit user opt-in on our website and that is only for customer acquisition - no user data is ever monetized.

GDPR policy

Please find our GDPR Policy here: https://www.goosechase.com/privacy

Data Retention & Deletion

Defined data retention periods

Our accounts are designed to have a full history for ease of use. For the complete removal of information, the account would need to be deleted.

Procedure upon termination of the service agreement

Users can request to have their data deleted at any moment within the app, by sending an email to hi@goosechase.com or submitting a form through https://privacy.saymine.io/Goosechase_Adventures_Inc. Upon receiving a data deletion request, from the app, form or email, the user's third-party data will also be deleted (if applicable)

Before permanently deleting their data, users would be able to export their data, including any submissions (videos or photos) as well as the data gathered to date.

Deletion methodology

When we receive a request asking for total data deletion, we just wipe it out of our database, and from our backups. Our systems would also delete their data from other software in which their data may be held, such as Mixpanel or Intercom.

Backup deletion frequency

Backups are kept indefinitely unless a user specifically requests permanent data deletion. Upon receiving any data deletion requests, the process described above would also include data deletion from our backups.

Audit and Compliance

Assessing the application for security vulnerabilities prior to production deployment

As part of our development processes, we regularly audit all third-party libraries for updated versions and security patches. Our build process also automatically audits our libraries for known vulnerabilities. We also use automated vulnerability scanning and other manual testing.

Monitoring privacy breaches

We have intrusion sensors and 24x7 real-time automated monitoring systems for log-ins. We have a rotation system that ensures that someone can be paged and act upon any intrusion in the briefest delays. We also have log safeguards so that our CTO can go back historically in system and application logs to forensically identify the causes of a breach in both production and staging environments. Our incident response procedure may be shared upon contacting alex@goosechase.com

Security development

The application development follows OWASP top ten, and we follow industry best practices across the board.

Change Control

Logging activities & log safeguards

We have an automated monitoring system for log-ins, along with log safeguards so that one can go back historically in system and application logs to forensically identify the causes of breaches in both production and staging environments.

Frequency of back up of critical IT systems and sensitive data

Our backup is run automatically every 24hrs.

Change control process

We use a Git repository for tracking changes in any set of files, and we have the ability to do rollbacks on any changes performed.

Human Resources

Accountability for cyber security and security testing program

Logan Fuller, our CTO & CISO.

Security team

Logan is both our Chief Information Security Officer, as well as our Chief Technology Officer. He would report to the board, including Alyshahn, our CRO, and Andrew, our CEO. The security team currently comprises of Logan, Alexander (head of legal), and another senior engineer.

Team

We have a small team of developers. Duties are separated to reduce the opportunity for unauthorized modification, unintentional modification or misuse of the organization's IT assets.

Team training

Every team member is rigorously tested on these matters ahead of hiring and extensively trained throughout their onboarding period to cover all bases. Periodic training and continuous learning on security issues as well as other cyber security matters are also performed when and if needed.

Termination

Upon termination, employees are revoked access from all platforms as they are being communicated the information. Their access to their email, workspace, password manager, project management software, slack, and any other systems are simultaneously revoked. Upon termination, we always pay their termination notice forward so that they do not need to work for us in the interim.

Infrastructure and Virtualization Security

Segregation between production and non production environments

Both Production and non-production environments are entirely firewalled, one cannot access the other, making them entirely segregated.

Separation

System and network environments are both protected and separate by a firewall.

Identity and Access Management

Endpoint protection controls

We use firewall authentication and validation systems for every system connected to our infrastructure.

Restriction, log and monitoring access to our systems

All authentication attempts to our platform, successful or otherwise, are logged. We also fully log all requests to our service, though we do not specifically audit or log access to customer data or changes to security configurations.

Ensuring that access to data is granted on as needed basis

Team members do not have access to any user's unencrypted data unless explicitly required to perform a function that is a direct benefit to the user such as upgrading an account, an Experience or providing contextual support.

Do you use multi factor authentication for all privileged access?

Single sign-on protocols and multi-factor authentication are not currently supported.

Preventing unauthorized access to systems, applications, users' data or source code

One's data can be ingested via our website or mobile applications. In both interfaces, all requests require authorized accounts with the appropriate permissions for all data types and are carried out over TLS connections. We also rate-limit login attempts based on IP.

Process for granting and documenting approval for access of tenant data

Accounts are initially authorized via username/email and password combinations, with appropriate per-user API keys being returned for all future requests. All passwords are fully salted and hashed before being stored in our database and are never transmitted, stored, or logged in plaintext.

Incident Management

Incident management process

Our lengthy incident management documentation can be accessed by contacting alex@goosechase.com

Monitoring infrastructure for identification of events related to a specific users

Our monitoring infrastructure allows for the identification of events related to a specific user.

Enforcing and attesting to tenant data separation when producing data in response to legal subpoenas

Our head of legal operations would handle all subpoenas and/or court orders. Any process would follow and be aligned with any local jurisdictions, as well as our own in Ontario.

Contact in the unlikely event it would be needed

It's very likely that should any issues arise, our team will be aware of them and contact you proactively. However, if a security incident does arise and you need to contact us, you can contact our CRO directly at alyshahn@goosechase.com or 647 984 7806.

In the matter of a security incident, you can expect a response immediately. You will be made aware if there is a different point of contact at any point during the course of our partnership.

Integration

Ways to safe-list the application

IPs are 104.200.22.31 and 2600:3c00:1::68c8:161f, though ideally just safe-listing *.goosechase.com should do as we have a dynamic address.

Methods to integrate with other SaaS or on-premise systems

Direct API access.

RESTful APIs via an API Gateway

We don't use a Gateway but we can consume Restful API.

Method of sending email notifications (to registrants & staff) from this system

Email notifications are sent via Grid as well as Intercom.