Security Features

1. Product Information

- 1.1 What is Goosechase?
- 1.2 Types of Accounts
- 1.3 How is data being processed (i.e. who has access to customer data?)
- 1.4 Experience Privacy

2. Encryption

- **2.1 How is data encrypted?**
- **2.2 Backup encryption**
- **2.3 Crypto and key management scheme used**
- 2.4 How are admin systems accessed?

3. Server and Application Interface Security

- 3.1 Data location, access and storage
- 3.2 Ensuring that only tested and non-malicious code is released to production
- 3.3 Application and supporting infrastructure design
- 3.4 Application Distribution Security
- 3.5 Network Port for Server-Client Communication

4. Third Party

- 4.1 List of third parties that may have access to tenant data or any subset of the data
- 4.2 Do we share data?
- 4.3 Privacy Policy
- 4.4 GDPR policy
- 4.5 Cookie Policies

5. Data Retention & Deletion

- 5.1 Defined data retention periods
- 5.2 Procedure upon termination of the service agreement
- 5.3 Deletion methodology
- 5.4 Backup deletion frequency
- 5.5 Data deletion for larger organizations

6. Audit and Compliance

- 6.1 Assessing the application for security vulnerabilities prior to production deployment
- 6.2 Monitoring privacy breaches
- 6.3 Security development
- 6.4 SOC 2 alignment

7. Change Control

- 7.1 Logging activities & log safeguards
- 7.2 Frequency of back up of critical IT systems and sensitive data
- 7.3 Change control process

8. Human Resources

- 8.1 Accountability for cyber security and security testing program
- 8.2 Security team
- 8.3 Our team
- 8.4 Team training
- 8.5 Termination

9. Infrastructure and Virtualization Security

- 9.1 Segregation between production and non production environments
- 9.2 Separation

10. Identity and Access Management

- 10.1 Endpoint protection controls
- 10.2 Restriction, log and monitoring access to our systems
- 10.3 Ensuring that access to data is granted on as needed basis

10.4 Single Sign On

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

10.6 Process for granting and documenting approval for access of tenant data

10.7 Principle of Least Privilege

11. Incident Management

11.1 Incident management process

11.2 Monitoring infrastructure for identification of events related to a specific users

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

11.4 Contact in the unlikely event it would be needed

11.5 Incident Response Timelines

12. Integration

12.1 Ways to safe-list the application

12.2 Methods to integrate with other SaaS or on-premise systems

12.3 RESTful APIs via an API Gateway

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

1. Product Information

1.1 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.

1.2 Types of Accounts

a. **Play as Guest;**

   The Play as a Guest option allows users to join an experience 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.

   As such, through this option, no Personally Identifiable Information is requested or collected from a User.

b. **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, choose their password, and add their email address. No other personally identifiable information will be requested to either create or maintain an account.

c. **Sign in with SSO**
   For organizations that prefer to manage authentication through their existing identity provider, Goosechase Studio supports Single Sign-On (SSO) for creator and admin accounts via SAML and OIDC. K-12 customers can also use Clever SSO, and participants can sign in to the mobile apps using Google SSO. Where SSO is used, account credentials and authentication are managed by the identity provider, and only the information necessary to provision and link the account (such as email address and display name) is collected by Goosechase. See section 10.4 for more details.

1.3 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.

1.4 Experience Privacy

Experience Privacy

When designing and creating an experience, users have the option to set their experience to "Hidden from Search Results", making it accessible only via a Join Code. Alternatively, users can choose "Available in Search Results", allowing others to discover the experience using either the experience name or the Join Code.

To provide an additional layer of privacy, experience creators can choose to add a password to their experiences, ensuring that only users with the password can gain access.

2. Encryption

2.1 How is data encrypted?

All customer data is encrypted during Transit and at Rest using TLS and SSL, with passwords salted and hashed.

2.2 Backup encryption

Backups are encrypted in transit and at rest using AES-256 encryption and SHA-256 hashing.

2.3 Crypto and key management scheme used

Passwords are salted and hashed.

2.4 How are admin systems accessed?

Access to administrative consoles for our cloud infrastructure (AWS) requires 2FA. Access to internal admin tooling, reporting systems, and the staging environment is gated behind dedicated AWS Client VPN endpoints — legacy bastion-server access has been retired in favour of this VPN-based model.

We operate separate AWS Client VPN endpoints for production and staging environments to ensure environment isolation; these endpoints are mutually exclusive — users must disconnect from one environment before establishing a connection to the other to prevent cross-environment access and maintain security boundaries. Production VPN sessions auto-terminate after 8 hours.

Authentication to the VPNs uses mutual TLS, with each user issued a unique X.509 client certificate distributed securely through our enterprise password manager. Certificates can be revoked individually via the AWS Client VPN certificate revocation list (CRL), enabling immediate access removal for offboarded team members.

3. Server and Application Interface Security

3.1 Data location, access and storage

Our platform is hosted on AWS (US East 2). We maintain strict environment separation with our staging environment operating in complete isolation from the production environment through physical segregation controls. The staging environment contains no customer data or production information.

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

We implement a comprehensive secure software development lifecycle with mandatory peer review processes and multi-layered validation controls prior to production deployment. All code commits undergo rigorous scrutiny through our established change management protocols.

Pre-deployment Security Controls:

1. **Mandatory Peer Code Review:** All code changes require approval from a minimum of one additional team member through pull request workflows
2. **Automated Testing Pipeline:** Continuous integration (CI) pipelines execute comprehensive unit test suites, integration testing, and static application security testing.
3. **Manual Quality Assurance:** Dedicated QA validation cycles including functional, regression, and security testing protocols
    - **Phased Deployment Strategy:** Canary deployment methodology enabling controlled rollout with immediate rollback capabilities
    - **Real-time Monitoring and Observability:** Application performance monitoring, centralized logging, error tracking, and exception monitoring systems provide continuous security posture assessment

3.3 Application and supporting infrastructure design

Our backend infrastructure now operates fully on AWS, utilizing S3 for scalable and resilient storage. We use EC2 to handle compute tasks, with IAM for detailed access control and security. Data security is maintained through in-flight encryption via TLS, alongside robust firewall rules, security groups, and VPC configurations for network isolation. For data durability and rapid recovery, we use S3 versioning and automated backups, ensuring reliable protection again data loss or corruption.

3.4 Application Distribution Security

We ensure the security of our application by distributing exclusively through trusted app stores like the Apple App Store and Google Play Store. This prevents unauthorized versions from being accessed, ensuring users always download the official, secure software. Updates are also distributed through these platforms, providing timely access to the latest security patches and features.

3.5 Network Port for Server-Client Communication

We use port 443 for server-client communication. This port is secured through encrypted HTTPS.

4. Third Party

4.1 List of third parties that may have access to tenant data or any subset of the data

We maintain contracts with each subprocessor to ensure compliance with data security and privacy standards. Our full subprocessor list, along with the purpose of each, is available at: https://www.goosechase.com/sub-processors

4.2 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. For the avoidance of doubt, no user data is ever sold to third parties.

4.3 Privacy Policy

Please find our Privacy policy here: https://goosechase.com/privacy

4.4 GDPR policy

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

4.5 Cookie Policies

Please find our Cookie Policy here: https://goosechase.com/cookie-policy

.

5. Data Retention & Deletion

5.1 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.

5.2 Procedure upon termination of the service agreement

Users can request to have their data deleted at any moment within the app, by;

- Deleting their account through the app
- Sending an email to hi@goosechase.com; or
- Submitting a form through https://privacy.saymine.io/Goosechase_Adventures_Inc.

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.

5.3 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.

5.4 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.

5.5 Data deletion for larger organizations

Under certain circumstances, we may agree to provide greater scope, control and granularity over data retention period and data deletion methodologies. Please contact our legal team for more information.

6. Audit and Compliance

6.1 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 automatically audits our libraries for known vulnerabilities via GitHub Dependabot, with critical findings tracked and remediated against defined SLAs. We also use Vanta for continuous compliance monitoring across our infrastructure, which automatically surfaces configuration drift and security findings into our remediation workflow. In addition, we use automated vulnerability scanning and manual testing to assess the application prior to production deployment.

6.2 Monitoring privacy breaches

We have intrusion sensors and 24×7 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 Principal Infrastructure & Security Engineer 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

6.3 Security development

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

We integrate accessibility best practices throughout our development process. We utilize internal checklists at each stage of development to ensure that Goosechase is an accessible platform for all users. A full Voluntary Product Accessibility Template can be requested by contacting our team

6.4 SOC 2 alignment

Our security program is being built to align with the SOC 2 Type II Trust Service Criteria. We use Vanta for continuous compliance monitoring, with our operational policies, vendor risk reviews, access controls, and onboarding/offboarding workflows operating as auditable processes. We are actively working towards a SOC 2 Type II audit — for the most current status, please contact our team at hi@goosechase.com.

7. Change Control

7.1 Logging activities & log safeguards

We use a combination of automated monitoring and AWS-native logging services. AWS CloudTrail records administrative and API activity across our infrastructure, VPC Flow Logs capture network traffic across our production VPCs, and our application records authentication attempts and service requests. These logs are retained with appropriate safeguards so that we can go back historically in system, application, and infrastructure logs to forensically identify the causes of breaches in both production and staging environments.

7.2 Frequency of back up of critical IT systems and sensitive data

We use AWS-native backup services with continuous data replication and automated recovery capabilities.

7.3 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.

8. Human Resources

8.1 Accountability for cyber security and security testing program

Alexandre Stylianoudis, our VP Legal & Finance; and

Jamieson Hale, our Principal Infrastructure & Security Engineer.

8.2 Security team

1. Jamieson Hale - Principal Infrastructure & Security Engineer
2. Alexandre Stylianoudis - VP Legal & Finance

8.3 Our 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.

8.4 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.

8.5 Termination

Upon termination, all logical access is revoked in line with our Employee Termination & Offboarding Information Security Policy. For involuntary terminations, all logical access is disabled immediately upon delivery of the termination decision; for voluntary terminations, no later than 48 hours after the final working day. Access to sensitive systems and Slack is disabled immediately in all termination scenarios, and physical access (badges, keys, office entry) is revoked at the termination meeting or end of the final working day, whichever comes first.

Access revocation covers identity provider accounts and SSO-connected apps, email, chat and collaboration platforms, source code repositories, CI/CD, cloud infrastructure, finance, CRM, HRIS, payroll, data warehouses, and any third-party

tools provisioned to the individual. Where BYOD is permitted, company data and profiles are removed via MDM. Continuing confidentiality, IP, and other post-termination obligations are reiterated in writing at termination, and completed offboarding checklists and revocation logs are retained for audit with quarterly compliance reviews.

Where applicable, we also pay terminated employees' notice period forward so that they do not need to work for us in the interim.

9. Infrastructure and Virtualization Security

9.1 Segregation between production and non production environments

Our organization maintains strict environment isolation through AWS-native security controls and network segmentation. Production and non-production environments operate in completely separate AWS Virtual Private Clouds (VPCs) with, amongst other things, the following security boundaries;

- Network-Level Isolation
- Access Control Segregation
- Physical Infrastructure Separation
- Security Group and NACL Controls
- IAM Role Separation

9.2 Separation

Our infrastructure implements defense-in-depth security through multiple layers of AWS managed and custom security controls:

- VPC Network Segmentation
- Application-Level Security
- Multi-Zone Architecture
- AWS Security Services Integration
- Zero-Trust Network Model

10. Identity and Access Management

10.1 Endpoint protection controls

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

10.2 Restriction, log and monitoring access to our systems

All authentication attempts to our platform, successful or otherwise, are logged, and we fully log all requests to our service. In addition, AWS CloudTrail records administrative and API activity across our infrastructure, including changes to security configurations, and VPC Flow Logs capture network traffic across our production VPCs. These logs are retained for forensic, audit, and compliance purposes.

10.3 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.

10.4 Single Sign On

Single Sign-On (SSO) is supported. Goosechase Studio offers SSO for creator and admin accounts via SAML and OIDC, allowing authentication against your organization's existing identity provider. K-12 customers can additionally use Clever SSO, and participants can sign in to the mobile apps using Google SSO. SSO for creator and admin accounts is available on select plans. Please contact our team at hi@goosechase.com for more information.

10.5 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.

10.6 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.

10.7 Principle of Least Privilege

At Goosechase, we adhere to the Principle of Least Privilege. Employees are granted access strictly based on the specific requirements needed to perform their job functions. This ensures that each individual has only the necessary permissions to carry out their responsibilities.

11. Incident Management

11.1 Incident management process

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

11.2 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.

11.3 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, Canada.

11.4 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, or our VP Legal & Finance at alex@goosechase.com or 323 916 4130.

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.

11.5 Incident Response Timelines

Incidents are categorized by severity, each with specific response and resolution times. See below for the incident types and their corresponding response and resolution details:

- Emergency Incident: Partially prevents or severely impairs platform usability and operations.
    - Response: Same day (EST hours);
    - Resolution: Starts within one business day.
- High Priority Incident: Limits usability but doesn’t prevent it, impacting productivity.
    - Response: Within one business day;
    - Resolution: Starts within two business days.
- Normal Priority Incident: Impairs services with limited operational impact.
    - Response: Within three business days;
    - Resolution: Initial response within five business days.
- Minor Priority Incident: Minimally impacts operations, not significantly impairing usability.
    - Resolution: Addressed in the next release.

12. Integration

12.1 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.

12.2 Methods to integrate with other SaaS or on-premise systems

Direct API access.

12.3 RESTful APIs via an API Gateway

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

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

Email notifications are sent via SendGrid as well as Intercom.