trivie

A Buyer's Guide for Security, Risk, and Compliance

Last Updated August 2021

All Information Considered Private and Confidential

Introduction

Who We Are

Trivie makes learning more engaging, measurable, and effective. Our SaaS-hosted web application, and complimentary Android and iOS native applications, serves as a training solution that uses gamification, artificial intelligence, and analytics to make learning initiatives more personalized and accessible.

Our Security Mission

Trivie's security mission is to protect our customers, their users, and our partners, safeguarding their data through best-in-class security.

In a world of data breaches and cyber attacks, we understand the risk that comes with sharing your information and we know how important it is to keep it safe, which is why we don't rely on a single layer of defense. From scanning to testing, our security program is based on defense in depth with multilayered security controls. We comply with privacy regulations and draw on best practices from SOC2 and NIST information security compliance frameworks. We take every possible step to keep your information and data safe.

This guide to security at Trivie outlines our approach to adhering to these principles and our commitment to continually reviewing, adapting, and improving our security posture.

Quick Reference

GPR Compliant
We comply with the European Union General Data Protection Regulation in the way we store, retrieve, and protect your data.

SOC 2 Compliance
We are currently working towards full SOC 2 Type II compliance.

Trivie is hosted on:

aws

All AWS servers are encrypted with AES-256

All data in transit and at rest is encrypted via SSL/TLS 1.2

The Data We Store & Processs

User Information

We realize that most security, privacy, compliance, and risk programs start by understanding what data we store, handle, and process. Since Trivie is used to engage individuals (employees, customers, contractors, or similar carbon-based lifeforms), demographic data is leveraged by our customers to garner deeper insights and reporting. For convenience, here is a list of common demographic elements customers provide to us, with required ones indicated with a *.

Note on GDPR: We fully comply with GDPR.

- First Name*
- Last Name*
- Work Email Address*
- Business Unit
- Locaton
- Division
- Department
- Manager Name
- Employee ID
- Employee Type

Since the demographic information sampled above powers administrator reporting, it's important that the business contacts using Trivie help identify the data fields necessary for their reporting needs.

User Information

- The following transfer mechanisms can be used to provision user accounts:
- Automated transfer via SFTP (customer or Trivie hosted; variable transfer frequencies)
- Direct integrations with HRIS systems (e.g. Active Directory, ADP, Workday, etc.)
- Bulk file imports (performed by the customer or Trivie)

Our People & Security Culture

Standards

Security starts and ends with people. World-class technology, the best providers, and bullet-proof processes are only as strong as the behaviors, practices, and readiness of the people supporting them. It's with this in mind that we take extra care when it comes to your security and our people.

To create a structure of accountability, we set up an infosec team to continually review and improve our information security, and help our people understand their role in maintaining our strong security posture. Led by our Head of Technology, the team is also supported by our experienced leaders across the company, from engineering, product, and executive management.

How Our People Keep Your Data Safe

All employees of Trivie, Inc. do the following:

- Sign confidentiality agreements that include customer information
- Sign our Code of Conduct that includes security and privacy policies
- Receive annual training in security and privacy, including best security practices, information on new threats and vulnerabilities, as well as privacy and legal/regulatory issues
- Use our own app, Trivie, to regularly reinforce security best practices and proactively inform and train employees on new global security threats and phishing trends
- Have an established and reviewed process to report any anomalies to a dedicated team that monitors regulatory and legal requirements, as well as current worldwide security events and trends

Our Hosting & Environment

Trivie is hosted on Amazon Web Services (AWS), the industry-leading provider that sets the bar for security best practices. AWS is recognized for data centers that are built to withstand all types of threats and are certified for high quality and security. Our engineering team also uses best-in-class tools for vulnerability scanning, malicious activity detection, and blocking suspicious behavior automatically.

- We use storage infrastructure designed for mission-critical and primary data storage, and AWS guarantees reliable data storage.
- All AWS servers are encrypted with AES-256.
- Enterprise customers are provisioned a single-tenant database.
- We take backups that are stored on multiple devices across multiple facilities in multiple availability zones. Daily backups ensure we can restore your data in case of failure or accidental deletion.
- All files that admins upload are stored on servers that use the latest techniques to remove bottlenecks and points of failure.
- We use different storage for user and application data. These servers are not exposed anywhere but the internal network, which is isolated from the internet.
- We use load balancers to ensure Trivie is online even with high traffic. Load balancers distribute requests to multiple servers, and this protects against attacks like DDoS.
- Database instances are only accessible via application systems within a private subnet.
- Database authentication credentials are system-generated and stored securely.
- User passwords are stored using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST.
- Trivie runs behind a firewall and is updated regularly with the latest security patches.
- Entire infrastructure utilizes intelligent threat detection and continuous monitoring for malicious or unauthorized behavior
- All information passed back and forth between our server and your computer is encrypted (SSL/TLS 1.2).
- We use in-depth monitoring services to visualize performance, detect irregular activity patterns, and ensure that our entire infrastructure is functioning as it should.

Our Policies

We have created comprehensive documentation, procedures, and policies as part of developing, maintaining, and growing our security posture.

- Access Control Policy
- Asset Management Policy
- Code of Conduct
- Cryptography Policy
- Data Management Policy
- Productivity Tools Policy
- Human Resources Security Policy
- Incident Response Plan
- Information Security Policy
- Information Security Roles and Responsibilities
- Operations Security Policy
- Physical Security Policy
- Risk Management Policy
- Secure Development Policy
- Third-Party Management Policy
- **Business Continuity and Disaster Recovery Policy:** We replicate data across separate, physically independent, and highly secure AWS locations, ensuring high availability, data integrity, and protection. Our comprehensive disaster recovery and business continuity plan can be provided upon request.
- **Data Retention Policy:** Trivie only keeps the data that is required to perform the service. Trivie does not and does not intend to sell your data. Your data will only be shared with any third parties that are required for Trivie to provide service (e.g. Amazon Web Services).
- **Data Deletion:** Customer database instances are destroyed upon the completion or termination of the business relationship between Trivie and the client. Backups of those database instances can remain available for up to 30 days, however, the deletion of those backups can be expedited upon request by the customer. Database backups are not guaranteed to be available upon completion of the business relationship.

Accessibility

Accessibility is a critical element of every successful product launch. Creating inaccessible products limits your user base, alienates some potential customers, and may open you up to legal liability. As such, Trivie has been concerned about accessibility from the beginning of our design process. Below we lay out the principles we've used to guide this accessible design process and suggests the next steps we'll take to keep getting better.

Our goal for has been to meet or exceed all AA WCAG Guidelines. We have focused on the following:

- **Text Alternatives**
  - Encourage users to upload alt text alongside images at every entry point.
  - Encourage users to caption their videos
- **Timing**
  - Timed quizzes are disabled by default
  - All videos and other time-based media include a scrobbler such that the user can approach the media at their own pace
- **Sequencing**
  - Pages are laid out in a predictable and clear manner to allow screen reader access
- **Distinguishability**
  - Colors are never used as the sole visual means of conveying information
  - Color contrasts meet AA or AAA requirements
  - Audio controllers are available for every audio player within the app
- **Input Assistance**
  - Errors are identified and suggested corrections are appended in all input fields.
  - Labels are available for all input fields.

In late 2021, we have an accessibility audit scheduled where we will work our way through the full WCAG2.1 Accessibility Quick Reference, updating all fields to AA or AAA WCAG guidelines.

trivie

Questions?

Reach us at hello@trivie.com