Security at Gorgias

Security is one of the top priorities for Gorgias because it's fundamental to your experience with the product. Gorgias is committed to securing your application's data, eliminating systems vulnerability, and ensuring continuity of access. Gorgias uses a variety of industry-standard technologies and services to secure your data from unauthorized access, disclosure, use, and loss. Security is directed by Gorgias's Chief Technology Officer. As part of our ongoing commitment to providing you the highest level of security assurance, Gorgias is SOC 2 Type 2 compliant.

This document aims to provide a high level overview of security efforts at Gorgias.

Enterprise Security

Policies

We've established a thorough set of security policies that are enforced by Gorgas' Security & Compliance teams. All security policies are reviewed and approved at least annually. Employees, interns, and contractors participate in mandatory security training when joining the company and through ongoing security awareness education.

People Security

Upon hire, each Gorgias employee is required to complete a background check, sign a security policy acknowledgment and non-disclosure agreement, and receive security training.
Individuals are granted access to the corporate and production systems, as required by their job responsibilities. In addition, all employees are required to complete annual security and privacy training, and they receive regular security awareness training via informational emails, phishing simulations, talks and presentations.

Workstation Security

Gorgias workstations are configured according to security best practices and are centrally managed. Workstations are required to run endpoint protection software and disk encryption. Access to workstations is secured with strong passwords and biometric authentication. Operating systems are configured to automatically apply security updates and patches to ensure workstations remain secure.

Corporate Offices

Physical access to corporate facilities, other than public entrances and lobbies, is restricted to authorized Gorgias personnel and registered visitors who are accompanied by Gorgias personnel. A badge access system ensures only authorized individuals have access to restricted areas within the corporate facilities.

Gorgias offices do not host any servers that process production customer data.

Infrastructure and Network Security

Physical Security

Gorgias is hosted on Google Cloud Platform. Google data centers feature a layered security model, including extensive safeguards such as:

- Custom-designed electronic access cards
- Alarms
- Vehicle access barriers
- Perimeter fencing
- Metal detectors
- Biometrics

Google's data centers are equipped with highly advanced intrusion detection systems, and are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by professional security guards who have undergone rigorous background checks and training. Google Cloud Platform

undergoes various third-party independent audits on a regular basis. This includes, but is not limited, to SOC 2 and ISO 27001 compliance.

Gorgias employees do not have physical access to Google data centers, servers, network equipment, or storage.

Network Access Control

Gorgias is the assigned administrator of its infrastructure on Google Cloud Platform, and only designated authorized Gorgias operations team members have access to configure the infrastructure on an as-needed basis behind a two-factor authenticated virtual private network. Specific private keys are required for individual servers, and keys are stored in a secure and encrypted location.

Application Security

As part of its comprehensive application security program, Gorgias has developed a set of security checks, throughout the software development lifecycle, to mitigate the risk of any vulnerabilities reaching our production systems.
This effort includes, but is not limited to first-party code static security scanning, code and system dependency scanning, as well as infrastructure-level scanning.

In addition to the aforementioned technical checks, Gorgias carries out systematic peer reviews of project designs, and code commits.

Third-Party Audits

To ensure Gorgias services' security adheres to widely recognised standards, Gorgias' security program includes annual grey box penetration testing as well as a private bug bounty program. This provides reasonable assurance that potential vulnerabilities would be caught before they can be exploited.

Business Continuity and Disaster Recovery

High Availability

Every part of the Gorgias service uses properly-provisioned, redundant servers (e.g., multiple load balancers, web servers, replica databases) in the case of failure. As part of regular maintenance, servers are taken out of operation without impacting availability.

Backups

Gorgias keeps continuous encrypted backups of data in multiple regions on Google Cloud Platform. In the case of production data loss (i.e., primary data stores lost), organizational data would be restored from these backups.

Incident Response

Gorgias has an established incident response plan that ensures timely identification, escalation, and resolution of security incidents. All incidents are thoroughly documented, investigated, and, where appropriate, post-incident reviews are conducted to drive continuous improvement.

As part of our incident response procedures, our engineering teams are trained to:

- Promptly respond to alerts of potential incidents.
- Determine the severity of the incident.
- If necessary, execute mitigation and containment measures.
- Communicate with relevant internal and external stakeholders, including notification to affected customers to meet breach or incident notification contractual obligations and to comply with relevant laws and regulations.
- Gather and preserve evidence for investigative efforts.
- Document a postmortem and develop a permanent triage plan.

Our incident response policies and processes are audited as part of our SOC 2 compliance audits.

Systems status live report

Gorgias maintains a live report of operational uptime and incidents on our public status page. Anyone can subscribe to updates via email from the status page. All known incidents are reported there.

Data Security

Data encryption

Encryption at rest

All data in Gorgias servers is encrypted at rest. Google Cloud Platform stores and manages data cryptography keys in its redundant and globally distributed Key Management Service. So, if an intruder were ever able to access any of the physical storage devices, the Gorgias data contained therein would still be impossible to decrypt without the keys, rendering the information a useless jumble of random characters. Encryption at rest also enables continuity measures like backup and infrastructure management without compromising data security and privacy.

Encryption in transit

Gorgias exclusively sends data over HTTPS transport layer security (TLS) encrypted connections for additional security as data transits to and from the application.

Data Retention & Removal

Read more about data privacy at Gorgias here.

Vulnerability Disclosure

If you would like to report a vulnerability or have any security concerns with a Gorgias product, please contact security@gorgias.com and refer to our public Vulnerability Disclosure Policy.