Highlevel Security and Compliance Overview

Last update July 2023

HighLevel

Table of Contents

Introduction

Our Company and Products

Developed for agencies by an agency, HighLevel's goal is to help marketing professionals and agencies reach and surpass their benchmarks for success. We believe in enhancing automation, improving communication, and boosting scalability in a consumer-friendly way, and we consistently provide future-embracing updates that exemplify these priorities.

Since its inception in 2018, HighLevel has continuously grown exponentially, increasing the impact created on the tech community and the SaaS industry. At HighLevel, we measure our success by the successes of our customers and therefore prioritize optimizing our offerings in order to meet their needs.

Our AI-powered all-in-one sales, marketing, and customer relationship management (CRM) platform offers numerous features that are essential to agencies and marketers. This expansive software solution provides limitless opportunities for our customers to set lofty sales goals and actually achieve them while being supported by our team of experts. We also encourage our customers to rebrand our platform as their own, truly offering agencies and marketers everything they need to scale beyond what they ever thought possible for themselves, their businesses, and their clients.

HighLevel Security and Risk Focus

HighLevel’s primary security focus is to safeguard our customers’ data. HighLevel has invested in the appropriate controls to protect and service our customers. This investment includes the implementation of dedicated corporate, product, and infrastructure security programs. Our Legal Team, in partnership with other departments, oversees the implementation of these programs.

Our Security and Compliance Objectives

We have developed our security framework using best practices for the SaaS industry. Our key objectives include:

- Customer Trust and Protection: deliver superior products and services while protecting the privacy and confidentiality of data
- Availability and Continuity of Service: ensure availability of the service and minimize risks to service continuity
- Information and Service Integrity: make sure that customer information is never corrupted or altered inappropriately
- Compliance with Standards: aim to comply with or exceed industry standard best practices.

HighLevel Security Controls

In order to protect the data that is entrusted to us, HighLevel utilizes layers of administrative, technical, and physical security controls throughout our organization. The following sections describe a subset of our most frequently asked questions about control.

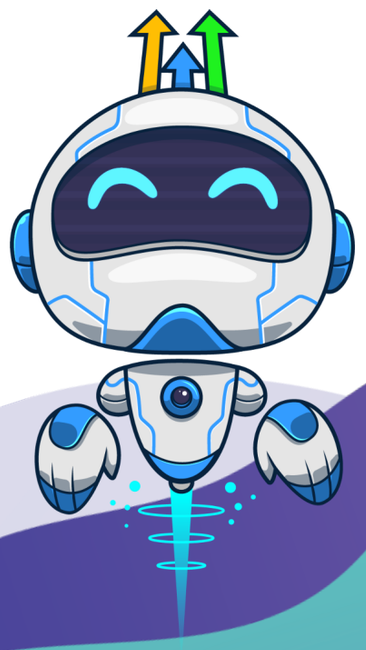
Infrastructure Security

Cloud Hosting Provider

HighLevel does not host any product systems or data within its physical offices. HighLevel outsources hosting of its product infrastructure to leading cloud infrastructure providers such as Google Cloud Platform Services and Amazon Web Services. Our product infrastructure resides in the United States. We place reliance on Google's and AWS's audited security and compliance programs for the efficacy of their physical, environmental, and infrastructure security controls.

Google provides a monthly uptime percentage to customers of at least 99.5%. You can find more information about the controls, processes, and compliance measures implemented by Google on their publicly available Compliance Resource Center.

AWS guarantees between 99.95% and 100% service reliability, ensuring redundancy to all power, network, and HVAC services. The business continuity and disaster recovery plans for the AWS services have been independently validated as part of their SOC 2 Type 2 report and ISO 27001 certification. AWS's compliance documentation and audit reports are publicly available at the AWS Cloud Compliance Page and the AWS Artifacts Portal.



Network and Perimeter

The HighLevel product infrastructure enforces multiple layers of filtering and inspection on all connections across our web application, logical firewalls, and security groups. Network-level access control lists are implemented to prevent unauthorized access to our internal product infrastructure and resources. By default, firewalls are configured to deny network connections that are not explicitly authorized. Changes to our network and perimeter systems are controlled by standard change control processes. Firewall rulesets are reviewed periodically to help ensure that only necessary connections are configured.

Configuration Management

Automation drives HighLevel's ability to scale with our customers' needs and rigorous configuration management is baked into our day-to-day infrastructure processing. The product infrastructure is a highly automated environment that expands capacity as needed. All server configurations are embedded in images and configuration files, which are used when new containers are provisioned. Each container includes its own hardened configuration and changes to the configuration and standard images are managed through a controlled change pipeline. Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. In the event that a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline within 30 minutes. Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline.

Logging

Actions and events that occur within the HighLevel application are consistently and comprehensively logged. These logs are indexed and stored in a central logging solution hosted in HighLevel's cloud environment. Security relevant logs are also retained, indexed, and stored to facilitate investigation and response activities. The retention period of logs depends on the nature of the data logged. Write access to the storage service in which logs are stored is tightly controlled and limited to a small subset of engineers who require access.

Alerting and Monitoring

HighLevel invests in automated monitoring, alerting, and response capabilities to continuously address potential issues.

The HighLevel product infrastructure is instrumented to alert engineers and administrators when anomalies occur. In particular, error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses or alerts to the appropriate teams for response, investigation, and correction. Many automated triggers are also designed to immediately respond to anomalous situations. For example, traffic throttling, process termination, and similar functions are triggered at predefined thresholds.

Application Security

Web Application Defenses

All customer content hosted on the platform is protected by firewall and application security. The monitoring tools actively monitor the application layer and can alert on malicious behavior based on behavior type and session rate. The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP), specifically the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure customers' web sites and other parts of the HighLevel products are continuously available.

Development and Release Management

HighLevel optimizes our products through a modern continuous delivery approach to software development. New code is regularly deployed. Code reviews, testing, and merge approval is performed before deployment. Static code analysis runs regularly against code repositories and blocks known misconfigurations from entering the code base. Approval is controlled by designated repository owners and once approved, code is automatically submitted to HighLevel's continuous integration environment where compilation, packaging and unit testing occur. Dynamic testing for security vulnerabilities is performed periodically against our applications. Newly developed code is first deployed to a dedicated and separate QA environment for the last stage of testing before being promoted to production. Network-level and project-level segmentation prevents unauthorized access between QA and production environments. All code deployments are automated and in case of failures, the changes can be reverted. The deploying team manages notifications regarding the health of their applications and if a failure occurs, rollback processes are immediately engaged. We use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch).

HighLevel features seamless updates and, as a SaaS application, there is no downtime associated with releases. Major feature changes are communicated through in-app messages and/or product update posts.

Vulnerability Management

The HighLevel team manages a multi-layered approach to vulnerability management, using a variety of industry-recognized tools and threat feeds to ensure comprehensive coverage of our technology stack. Vulnerability scans are configured to scan for vulnerabilities on a regular basis, using adaptive scanning inclusion lists for asset discovery as well as the latest vulnerability detection signatures. We perform annual penetration tests against our applications and infrastructures to identify vulnerabilities that may present security related risks. Relevant findings are assessed, and mitigations are prioritized accordingly.

Customer Data Protection

Data Classification

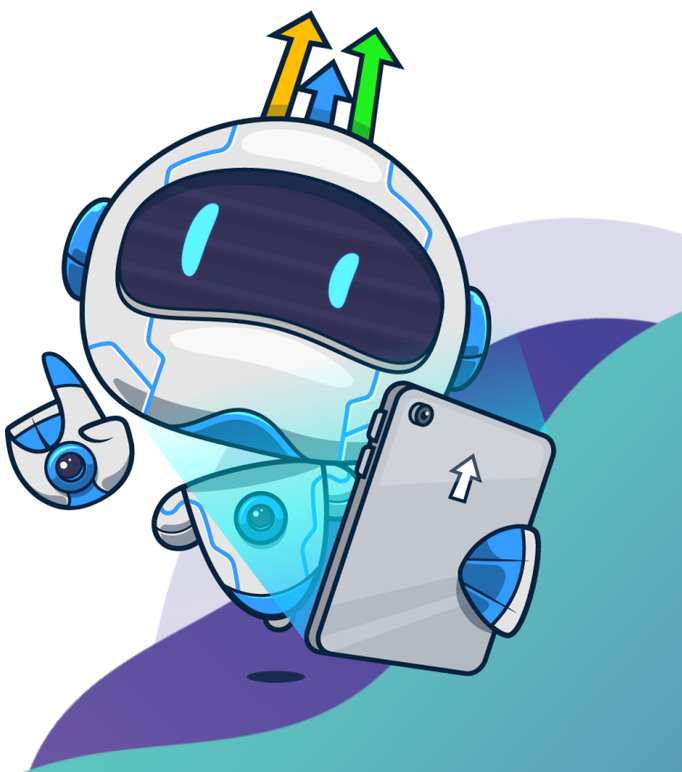
Per the HighLevel's Terms of Service, our customers are responsible for ensuring they only capture appropriate information to support their marketing, sales, services, content management, and operations processes. The HighLevel products should not be used to collect or store sensitive information, such as credit or debit card numbers, financial account information, Social Security numbers, passport numbers, financial or health information except as otherwise permitted.

Tenant Separation

HighLevel provides a multi-tenant SaaS solution where customer data is logically separated using unique IDs to associate data and objects to specific customers. Authorization rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes, application availability, and user access and changes are logged.

Encryption

All data is encrypted in transit with TLS version 1.2, or 1.3 and 2,048 bit keys or better. Transport layer security (TLS) is also a default for customers who host their websites on the HighLevel platform.



HighLevel leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices, and are encrypted at rest.

Key Management

Encryption keys for both in transit and at rest encryption are securely managed by the HighLevel platform. TLS private keys for in transit encryption are managed through our content delivery partner. Volume and field level encryption keys for at rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at varying frequencies, depending upon the sensitivity of the data they govern. In general, TLS certificates are renewed annually. HighLevel is unable to use customer supplied encryption keys at this time.

Data Backup and Disaster Recovery

System Reliability and Recovery

HighLevel is committed to minimizing system downtime. All HighLevel product services are built with redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a point in time recovery.

Back up Strategy

System Backups

Systems are backed up on a regular basis with established schedules and frequencies. Seven days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Backups are monitored for successful execution, and alerts are generated in the event of any exceptions. Failure alerts are escalated, investigated, and resolved. Data is backed up daily to the local region. Monitoring and alerting is in place for replication failures and triaged accordingly.

Physical Backup Storage

Because we leverage public cloud services for hosting, backup, and recovery, HighLevel does not implement physical infrastructure or physical storage media within its products. HighLevel does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.

Backup Protections

By default, all backups are protected through access control restrictions and write once read many (WORM) protections on HighLevel product infrastructure networks, and access control lists on the file systems storing the backup files.

Customer Data Backup Restoration

HighLevel customers don't have access to the product infrastructure in a way that would allow a customer-driven failover event. Disaster recovery and resiliency operations are managed by HighLevel product engineering teams. In some cases, customers can use the recycle bin to directly recover and restore contacts, opportunities, custom fields, custom values, tags, notes, and tasks up to 30 days after they were deleted. Changes to web pages, blog posts, or emails can be restored to previous versions of content using version history. For customers who wish to additionally back up their data, the HighLevel platform provides many ways of ensuring that you have what you need. Many of the features within your HighLevel portal contain export options, and the HighLevel library of public APIs can be used to synchronize your data with other systems.

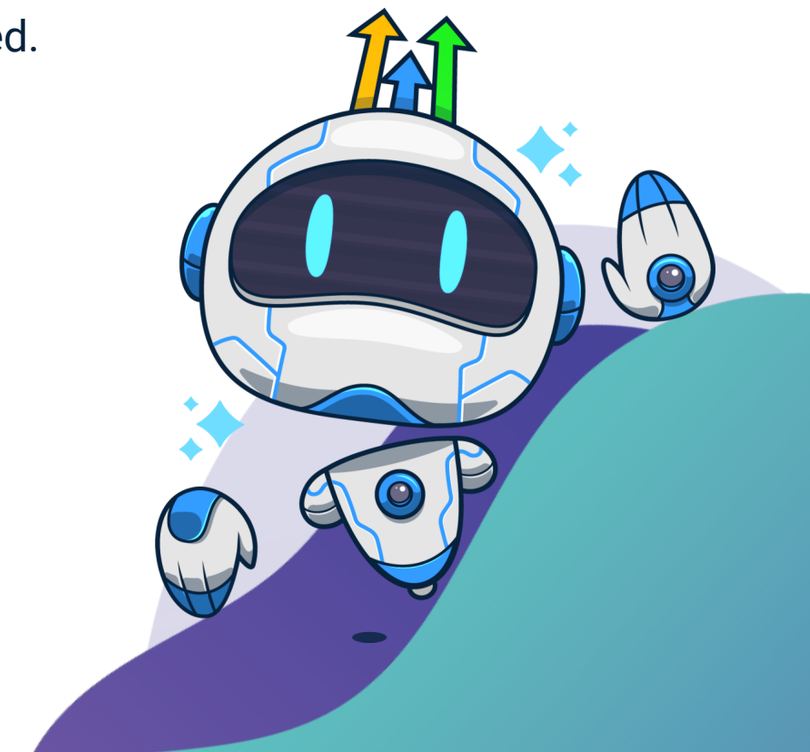
Identity and Access Control

Product User Management

The HighLevel products allow for granular authorization rules. Customers are empowered to create and manage the users in their portals, assign the privileges that are appropriate, and limit access as they see fit.

Product Login Protections

The HighLevel products allow users to login to their HighLevel accounts using the native HighLevel login. The native login enforces a uniform password policy which requires a minimum of 8 characters and a combination of lower and upper case letters, special characters,, and numbers. People who use HighLevel's native login cannot change the default password policy. Customers who use HighLevel's built-in login are protected by two-factor authentication for their HighLevel accounts. Portal administrators may require all users to have two-factor authentication enabled.



HighLevel Employee Access to Customer Data

Access to Production Infrastructure

User access to internal data stores and production infrastructure is strictly controlled. HighLevel employees are granted access using a role-based access control (RBAC) model. Day to day access is minimized to members of the Engineering team and persistent administrative access is restricted. Additionally, direct network connections to product infrastructure devices over SSH or similar protocols is prohibited, and engineers are required to authenticate first through a bastion host or "jump box" or have assigned IAM role to the resource before accessing server environments.

Access to Customer Portals

By default, Customer Support, Services, and other customer engagement staff can obtain limited access to parts of your HighLevel account to help you with using HighLevel. The HighLevel application also uses a JITA model to grant employees access to a customer's portal for a limited duration (Portal JITA). Each Portal JITA request is logged. Access is tied to a specific customer's portal for a maximum 24-hour period. HighLevel also utilizes risk-based monitoring to detect unusual Portal JITA activity.

When accessing a portal using Portal JITA, HighLevelers are unable to perform high-risk actions such as:

- Changing domain or SSO settings
- Exporting users/contacts
- Viewing/creating/deleting/rotating private app keys
- Importing data to the CRM
- Deleting contacts, companies, deals, and tickets

User logins, HighLevel employee access, security activity, and content activity is logged.

Corporate Authentication and Authorization

Access to the HighLevel company network requires MFA. Password policies follow industry best practices for required length, complexity, and rotation frequency. Password vaults are in place to manage certain administrative account passwords, and access to the vault is managed through Role Based Access Control or through the JITA process. We have built an extensive support system to streamline and automate our security management and compliance activities.

In addition to many other functions, we ensure that permission grants are appropriate, employee events are managed, access revocations are timely, change logs are effectively collected, and compliance evidence is preserved. Employee access and permissions to key internal systems are manually reviewed semi-annually to help ensure access granted is necessary for their job function.

Organizational and Corporate Security

Background Checks and Onboarding

HighLevel employees undergo a third party background check prior to formal employment offers. Reference verification is performed at the hiring manager's discretion. Upon hire, all employees must read and acknowledge HighLevel's Employee Handbook and Code of Conduct which help to define employee's security responsibilities in protecting company assets and data.

Policy Management

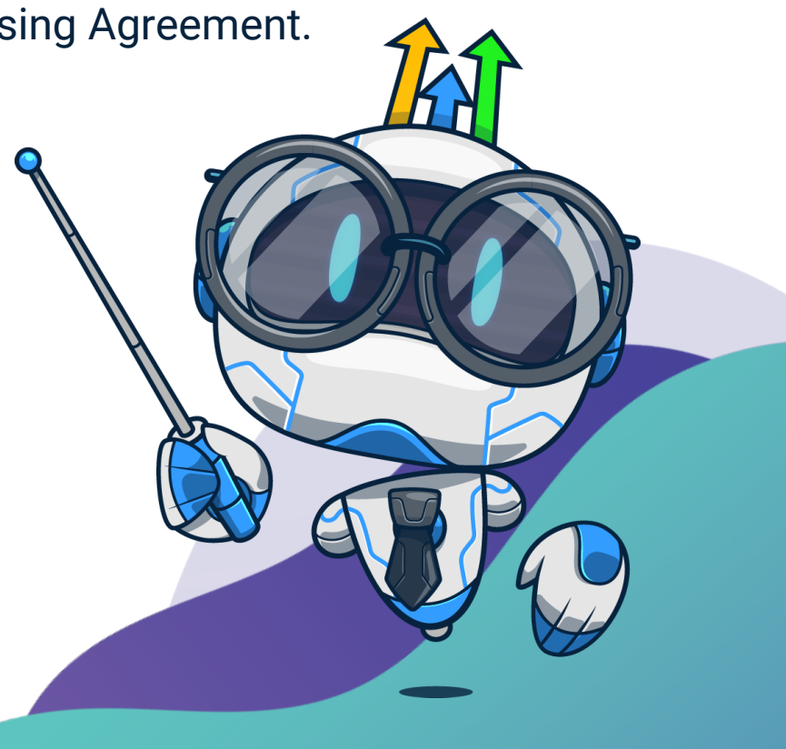
To help keep all our employees on the same page with regard to protecting data, HighLevel documents and maintains written policies and procedures. Specifically, HighLevel maintains a core Written Information Security Policy, which covers a variety of topics such as data handling requirements, privacy considerations, and disciplinary actions for policy violations. Policies are reviewed and approved at least annually.

Security Awareness Training

HighLevel employees are required to complete CyberSafety training when they start their employment, and training is made available annually thereafter. The CyberSafety training also includes phishing awareness.

Vendor Management

HighLevel may leverage third party service providers to support the development of our product as well as internal operations. We ensure that our vendors have appropriate security and privacy controls in place as part of our contractual relationship with them. We also maintain a list of our sub-processors (which may change from time-to-time) within our Data Processing Agreement.



Endpoint Protection

Company issued laptops are centrally managed and are configured to maintain full disk encryption. We implement a Mobile Device Management solution that provides a centralized platform for IT administrators to manage and monitor mobile devices in an organization. This includes configuring device settings, enforcing security policies, deploying apps, and ensuring compliance with corporate policies.

Compliance

Sensitive Data Processing and Storing

Please see our Terms of Service and Privacy Policy for additional information on how and why we process data. Please note that, while HighLevel customers may pay for services by credit card, HighLevel does not store, process, or collect credit card information submitted to us by customers, and we are not PCI-DSS compliant. We leverage PCI-compliant payment card processors to ensure that our payment transactions are handled securely.

Privacy

As described in our Privacy Policy, we do not sell your personal data to third parties. The protections described in this document and other protections that we have implemented are designed to ensure that your data stays private and unaltered.

Data Retention and Data Deletion

Customer data is retained for as long as you remain an active customer. Current and former customers can make written requests to have certain data deleted, and HighLevel will fulfill those requests as required by privacy rules and regulations. HighLevel retains certain data like logs and related metadata in order to address security, compliance, or statutory needs. HighLevel does not currently provide customers with the ability to define custom data retention policies.

Privacy Program Management

HighLevel's Legal Team collaborates with our engineering and product development teams to implement an effective privacy program. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy and Data Processing Agreement.

Breach Response

HighLevel will notify customers as required by law if it becomes aware of a data breach that impacts your personal data.

GDPR

HighLevel aims to provide features that enable our customers to easily achieve and maintain their GDPR compliance requirements. Please refer to our GDPR page for more information. While HighLevel seeks to enable your GDPR compliance efforts, use of the HighLevel product alone does not make you GDPR compliant.

Document Scope and Use

This document is intended to be a resource for our customers. It is not intended to create a binding or contractual obligation between HighLevel and any parties, or to amend, alter or revise any existing agreements between the parties. HighLevel is continuously improving the protections that we have implemented, so our procedures may be subject to change.

Contact Us

Questions about this document? We want to hear from you! You can reach as at legal@gohighlevel.com