bakertilly

Proprietary & Confidential

SUPERHUMAN

Platform System

SOC 3

Relevant to Security, Availability, Confidentiality, and Privacy

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations™

OCTOBER 1, 2025 TO MARCH 31, 2026

Superhuman Confidential
PROPIN - FOIA exempt

Table of Contents

I. Independent Service Auditor's Report **1**

II. Superhuman Platform Inc.'s Assertion **4**

Attachment A - Superhuman Platform Inc.'s Description of the Boundaries of Its Platform System **5**

A. System Overview **5**

1. Services Provided 5
2. Infrastructure 7
3. Software 8
4. People 10
5. Data 12
6. Processes and Procedures 12

B. Complementary Subservice Organization Controls **13**

Attachment B – Principal Service Commitments and System Requirements **14**

Superhuman Confidential
PROPIN - FOIA exempt

I. Independent Service Auditor's Report

Superhuman Platform Inc.
2261 Market Street, Suite 85232
San Francisco, CA 94114

To the Management of Superhuman Platform Inc.:

Scope

We have examined Superhuman Platform Inc.'s accompanying assertion in Section II titled "Superhuman Platform Inc.'s Assertion" (assertion) that the controls within Superhuman Platform Inc.'s Platform System (system) were effective throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*.

Superhuman Platform Inc. uses Amazon Web Services (AWS) for cloud infrastructure and hosting services (subservice organization). Superhuman Platform Inc.'s description of the boundaries of its system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Superhuman Platform Inc., to achieve Superhuman Platform Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Superhuman Platform Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Superhuman Platform Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved. Superhuman Platform Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Superhuman Platform Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Superhuman Confidential
PROPIN - FOIA exempt

Baker Tilly Advisory Group, LP and Baker Tilly US, LLP, trading as Baker Tilly, are members of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. Baker Tilly US, LLP is a licensed CPA firm that provides assurance services to its clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and consulting services to their clients and are not licensed CPA firms.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Superhuman Platform Inc.'s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Superhuman Platform Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Superhuman Confidential
PROPIN - FOIA exempt

Opinion

In our opinion, management's assertion that the controls within Superhuman Platform Inc.'s Platform System were effective throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Baker Tilly US, LLP

San Francisco, California
May 29, 2026

Superhuman Confidential
PROPIN - FOIA exempt

II. Superhuman Platform Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Superhuman Platform Inc.'s Platform System (system) throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved based on the trust services criteria. Superhuman Platform Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

Superhuman Platform Inc. uses Amazon Web Services (AWS) for cloud infrastructure and hosting services (subservice organization). The description of the boundaries of our system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Superhuman Platform Inc., to achieve Superhuman Platform Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Superhuman Platform Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Superhuman Platform Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Superhuman Confidential
PROPIN - FOIA Exempt

Attachment A - Superhuman Platform Inc.'s Description of the Boundaries of Its Platform System

A. System Overview

1. Services Provided

COMPANY OVERVIEW

Grammarly was founded in 2009 by Max Lytvyn, Alex Shevchenko, and Dmytro Lider to help people communicate more effectively and has grown from a grammar and spelling tool into an AI-powered writing assistant that supports complex aspects of language and communication. Coda was founded in 2014 by Shishir Mehrotra and Alex DeRuiter, offering a collaborative, all-in-one platform that combines the features of documents, spreadsheets, and applications. Superhuman (now referred to as Superhuman Mail) was founded in 2014 by Rahul Vohra, Conrad Irwin, and Vivek Sodera, offering an AI-native email client that helps teams move through their inboxes faster and communicate more effectively.

In January 2025, Grammarly acquired Coda. In July 2025, Grammarly acquired Superhuman. The combined entities now operate as Superhuman Platform Inc. Superhuman Platform Inc. (Superhuman) was formed by combining two complementary technology companies.

Superhuman is headquartered in San Francisco, California, with offices in Mountain View, California; New York, New York; Seattle, Washington; Kyiv, Ukraine; Vancouver, Canada; Berlin, Germany; and Warsaw, Poland. Superhuman's mission-driven team is connected by its six core values:

- (Super) Human-Centered
- Win with Grit
- Craft Remarkable Delight
- Think from First Principles
- Grow Ideas from Anywhere
- Prioritize the Pond

Team members are deliberate about applying these values to everything Superhuman does, whether it is committing to an inclusive and learning-oriented work environment, supporting users with compassion and integrity, or thoughtfully creating secure products that connect people. Superhuman continues to invest in language research and collaborative productivity, backed by over $1 billion in financing led by General Catalyst, including a Customer Value Fund financing announced in May 2024.

Superhuman Confidential
PROPIN - FOIA Exempt

SYSTEM DESCRIPTION

Superhuman offers a comprehensive suite of productivity and communication tools across four integrated product lines:

- *Grammarly* – Grammarly, part of Superhuman's AI productivity suite, is an AI-powered writing assistant that provides real-time suggestions for correctness, clarity, engagement, and delivery across more than 1 million apps and websites. Available via browser extensions, desktop applications for Windows and Mac, and integrations with Microsoft Office apps including Word, Outlook, Teams, PowerPoint, and Excel, Grammarly helps over 40 million people and 50,000 organizations communicate more effectively. Enterprise customers benefit from advanced administrative controls, brand style guides and tone profiles, and organization-wide writing consistency features.
- *AI Editor* – The AI Editor is Superhuman's web-based text editor: a central writing environment where users can compose, revise, and collaborate on documents. Users can customize the types of writing suggestions they see based on their goals, access generative AI capabilities powered by third-party Large Language Model (LLM) providers (including Azure OpenAI, OpenAI, and Anthropic), and leverage advanced features such as tone detection, full-sentence rewrites, and plagiarism detection.
- *Superhuman Go* – Superhuman Go is a context-aware AI assistant that lives in users' browsers and helps them move faster across tools (email, docs, tickets, etc.) from a single sidebar/notch experience. Each Superhuman Go agent can help perform tasks, organize information, and deliver quick summaries so users can focus on higher-value work.
- *Superhuman Docs (Coda)* – Superhuman Docs is a collaborative, all-in-one platform that combines features of docs, spreadsheets, and applications. It includes powerful docs for creating, editing, and sharing content; relational tables for organizing and manipulating data; a formula language for automating complex operations; Packs for integrating with external applications; Workspaces for team-based collaboration; and an AI Assistant for generating, summarizing, and modifying content.

SYSTEM BOUNDARIES

The system boundaries considered in this report include the production systems, infrastructure, software, people, procedures, and data that support the Superhuman product lines described above.

SUBSERVICE ORGANIZATIONS

Superhuman uses Amazon Web Services (AWS) for cloud infrastructure and hosting services. This subservice organization is excluded from the scope of this report.

In-scope Superhuman server infrastructure is hosted in AWS data centers in the United States, in the US East (Northern Virginia) and US West (Oregon) regions.

As an infrastructure provider and solutions partner, AWS helps Superhuman ensure the scalability, availability, and durability of its platform and services.

Superhuman Confidential
PROPIN - FOIA exempt

2. Infrastructure

Superhuman's System is a web-based Software-as-a-Service (SaaS) system. The primary components of the System are built on top of AWS and hosted in data centers in the United States, in the US East (Northern Virginia) and US West (Oregon) regions. As an infrastructure provider and solutions partner, AWS helps Superhuman in supporting the scalability, availability, and durability of Superhuman's platform and services.

Superhuman is registered for an enterprise support plan, which provides rapid response from the AWS team. A signed contract between AWS and Superhuman is maintained to ensure fulfillment of the agreed responsibilities. As part of the plan, AWS provides consulting support to Superhuman's engineering teams regarding specific use cases and applications. This high-touch support also includes design reviews and architectural guidance.

The following AWS services are utilized:

- *Computing* – AWS Elastic Compute Cloud (EC2), AWS Lambda
- *Container Orchestration* – AWS Elastic Container Service (ECS), AWS Elastic Kubernetes Service (EKS)
- *Databases* – AWS DynamoDB, AWS Relational Database Service (RDS), AWS ElastiCache, AWS Redshift
- *Distributed Denial of Service (DDoS) Protection* – AWS Shield Advanced
- *Network* – Virtual Private Clouds (VPCs), Security Groups, Network Access Control Lists (ACLs)
- *Storage Services* – AWS Simple Storage Service (S3), AWS EBS

PRINCIPAL ARCHITECTURE

Superhuman's product infrastructure comprises the following main components:

WRITING ASSISTANCE ARCHITECTURE:

- Client Apps are Superhuman's product offerings that can be installed and used on different platforms.
- Load Balancer and Web Application Firewall are AWS services that distribute traffic across multiple servers to increase capacity and reliability and filter, monitor, and block traffic.
- Authentication API, Document Editor API, and Processing API are application programming interfaces that facilitate interaction between users and relevant Superhuman services.
- Authentication Service authenticates end users via login/password, single sign-on (SSO) via SAML OIDC, and social sign-on. Employee access to internal systems is managed through a separate corporate identity provider.
- AI Editor Service enables users to create, edit, and save documents.
- Processing Service and Specialized Processing Services manage connections from client apps (such as the browser extension and mobile keyboard) to provide writing suggestions.
- Azure OpenAI, OpenAI, and Anthropic are third-party LLM providers that enable the generative AI capabilities in Superhuman's product offering. The scope of the report does not include the evaluation of the performance or integrity of third-party LLM providers or the services they provide.

Superhuman Confidential
PROFIT - FOIA exempt

COLLABORATIVE PLATFORM ARCHITECTURE:

- The Superhuman Docs Platform comprises native AWS infrastructure resources, custom microservices, and a web-based front-end.
- The network infrastructure layer that logically isolates the resources and network used by the Platform.
- The Platform enables users to create, edit, and collaborate on docs, tables, formulas, and applications through a web-based interface.

AI ASSISTANT ARCHITECTURE:

- The Superhuman Go Platform comprises native AWS infrastructure resources, custom microservices, and a web-based front-end (including a browser extension and in-app surfaces).
- The network infrastructure layer that logically isolates the resources and network used by the Platform.
- The Platform enables users to invoke AI agents that read context from active applications, take actions on the user's behalf, and orchestrate multi-step workflows across connected tools through a web-based interface.

3. Software

The System is composed of native AWS infrastructure resources, custom microservices, and web-based frontends. The infrastructure layer includes restrictive VPCs encapsulating the resources and networks used by the Superhuman Platform System.

When procuring third-party services and products that may affect the information security of Superhuman assets, Superhuman conducts vendor and system security risk assessments to understand associated risks and confirm that safeguards and controls are in place.

SUPPORTING SOFTWARE, SERVICES, AND TOOLS

The table below lists the software, services, and tools that support Superhuman's control environment and customer offerings.

Component	Service
Bug Bounty Platform	HackerOne
Code and Release Management	GitLab, GitHub, Artifactory
Computing	AWS EC2, AWS Lambda
Container Orchestration	AWS ECS, AWS EKS
Corporate Asset Management	JAMF, Workspace One
Corporate Communication	Google Workspace, Slack, Zoom

Superhuman Confidential
PROPIN - FOIA exempt

Component	Service
Customer Management	Salesforce
Customer Support System	Zendesk
Databases	AWS DynamoDB, AWS RDS, AWS ElastiCache, AWS Redshift
DDoS Protection	AWS Shield, AWS Shield Advanced
Endpoint Protection	CrowdStrike
Hiring	Greenhouse
Hosting	AWS S3, AWS EBS
HRIS/Talent Performance	Workday
Identity and Access Management	Okta, Opal
Learning and Development	Sana
Log Management and SIEM	Sumo Logic, AWS CloudTrail
Monitoring	AWS CloudWatch, PagerDuty, Grafana
Password Management	1Password
Payment System	PayPal, Braintree, Stripe
Secure Remote Access	Cloudflare Zero Trust
Storage Services	AWS S3, AWS EBS
Team Collaboration	Superhuman Docs, Atlassian Jira, and Confluence Cloud
Vendor Management	Onspring
Vulnerability Management	Detectify was decommissioned and replaced by Escape in January 2026

Superhuman Confidential
PROPIN - FOIA exempt

A variety of additional SaaS systems listed in the overview above are also managed by third-party vendors and are used by Superhuman, including PayPal, Braintree, Stripe, and Salesforce, among others. These vendors are support tools that do not impact Superhuman's ability to meet the trust services criteria.

4. People

The control framework that supports Superhuman's organizational environment starts with its Executive team. The following are key roles involved in control implementation and maintenance:

- Chief Technology Officer (CTO)
- General Counsel (GC)
- Chief Information Security Officer (CISO)

The CISO is responsible for managing security (confidentiality, integrity, and availability) and privacy across the organization. The CISO acts as the Information Security and Privacy Management System (ISPMS) Manager and oversees the ISPMS operations.

In addition to the overall governance provided by the Executive team, the following teams play a key role in the execution of controls:

- *Engineering* – The Engineering team is responsible for software development and for building and supporting the product ecosystem. This team also includes the Privacy & Responsible AI (RAI) team.
- *Security* – The Security team is responsible for securing applications and service data, comprising five sub-teams: Corporate Security, Product Security, Platform Security, Detection and Response, and Security Intelligence.
- *Human Resources (HR) / People* – Responsible for employee onboarding, setting policies, employee reviews, hiring processes, learning and development, compensation and benefits, and diversity and inclusion programs.
- *Corporate Systems* – Builds and supports enterprise infrastructure, focusing on identity and access management, corporate networks, and endpoint security. Includes Corporate Systems and IT teams.
- *Legal* – Provides legal review and support for privacy-related aspects of the product ecosystem and global company policies.
- *Governance, Risk, and Compliance (GRC)* – Establishes and coordinates security processes and practices across the organization in compliance with industry security standards.
- *Customer Support* – Provides support for customers' needs at the forefront of every interaction.

The following teams are relevant for this report:

- *Board of Directors* – Responsible for establishing and overseeing the company's strategy.
- *Executive* – Responsible for overseeing company operations.

Superhuman Confidential
PROPIN - FOIA exempt

- *Security* – Comprises five sub-teams responsible for ensuring security across the company.
  - *Corporate Security* – Manages security for Superhuman's corporate environment, including oversight of change management safeguards, security alerting, and validation of security controls across the organization.
  - *Product Security* – Collaborates with Superhuman Engineering to share advanced security expertise and help ship product offerings with industry-level application security.
  - *Platform Security* – Builds and supports the production infrastructure's security, focusing on the cloud and data platform.
  - *Detection and Response* – Support Superhuman's security program by owning monitoring tools and security incident response.
  - *Security Intelligence* – Enhances security prioritization by proactively generating and processing information from diverse sources to identify, prioritize, and mitigate potential threats to Superhuman assets.
- *Legal* – Provides legal review and support for privacy-related aspects of Superhuman's product ecosystem and global company policies.
  - *GRC* – Establishes and coordinates security processes and practices across the organization in compliance with industry security standards.
- *Developer Experience and Cloud Infrastructure* – Considers custom requirements and constraints to provide an optimal company-wide infrastructure toolkit that helps engineers focus on product development and maximize value for end users.
- *Privacy & Responsible AI* – Ensures responsible development and deployment of AI capabilities across Superhuman's product ecosystem, including governance of AI model usage, data privacy practices, and Responsible AI standards.
- *Engineering Organization* – A collaborative group of technical teams responsible for building and supporting Superhuman's product ecosystem.
- *Corporate Systems* – Builds and supports enterprise infrastructure, focusing on identity and access management, corporate networks, and endpoint security.
  - *IT* – Assists with hardware issues, software licensing and management, office network, laptop support, and other IT-related requests.
- *People* – Comprises multiple teams delivering company-wide programs and solutions for Superhuman's team. The People Operations, the Learning and Development team, and the People Partners address organizational learning needs, deliver benefits and team support systems, develop and manage people programs, implement global compensation and benefits strategies, manage diversity and inclusion programs, and provide coaching and partnership solutions to meet business needs. The Recruiting team oversees Superhuman's hiring processes and operations.
- *Customer Support* – Provides timely, empathetic help that keeps the customer's needs at the forefront of every interaction.

Superhuman Confidential
PROPIN - FOIA exempt

5. Data

Within the System, customer data is any information users provide in connection with their use of the service, including personal information provided during registration, such as name, email address, and password. Service data also includes any information users create, files users transmit or upload, and documents, data, or information generated or used in connection with the service. Payment information collected in connection with a purchase or payment, as well as information provided to Superhuman as part of an inquiry, is also included.

Customer data is segregated within the multi-tenant SaaS environment. The company's SaaS platform is built on third-party cloud service providers (AWS) and leverages their native isolation capabilities to prevent unauthorized cross-tenant access.

6. Processes and Procedures

Superhuman's GRC team maintains a Policy Central that contains documents required for performing security-related processes. Such processes include, but are not limited to, security risk assessment; information classification; and vendor, access, and change management. These documents range in level of detail, from policies defining the company's overall approach to managing a specific area to detailed guidelines providing specific instructions to responsible staff members.

Policies require approval by the ISPMS Manager and/or relevant functional heads. Such documents are reviewed annually or when there are relevant changes to existing processes, technologies, or organizational structure. Documents become effective when they are published to the organization. The portal is available to employees beginning their onboarding.

- Acceptable Use
- Access Management & Authentication
- Asset & Endpoint Management
- Business Continuity & Disaster Recovery
- Change Management
- Cryptography & Encryption
- Data Protection & Privacy
- Data Retention
- Information Classification
- Information Security & Privacy Management System (ISPMS)
- Human Resources & People
- Incident Response & Security Monitoring
- Legal & Regulatory Compliance
- Policy & Document Governance
- Risk Management
- Secure Development & Engineering
- Vendor Management
- Vulnerability Management

Superhuman Confidential
PROPIN - FOIA exempt

- Employee IT Lifecycle
- Customer Support

B. Complementary Subservice Organization Controls

Superhuman Platform Inc.'s controls related to the Platform System cover only a portion of overall internal control for each user entity of Superhuman Platform Inc.. It is not feasible for the criteria related to the Platform System to be achieved solely by Superhuman Platform Inc.. Therefore, each user entity's internal controls must be evaluated in conjunction with Superhuman Platform Inc.'s controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
Amazon Web Services	
1	Controls are in place and operating effectively to ensure environmental, geopolitical, business, and vendor risks are identified, evaluated, and addressed as part of service region, infrastructure, and third-party management processes.
2	Controls are in place and operating effectively to ensure logical access to AWS systems, networks, services, resources, and supporting infrastructure is appropriately authorized, provisioned, authenticated, reviewed, restricted, and timely revoked.
3	Controls are in place and operating effectively to ensure vulnerabilities and security events are identified, monitored, evaluated, escalated, and remediated in a timely manner.
4	Controls are in place and operating effectively to ensure encryption, key management, data handling, data disposal, and customer content deletion processes are implemented to protect customer information and render data unrecoverable when required.
5	Controls are in place and operating effectively to ensure physical access to AWS data centers and restricted server locations is authorized, monitored, periodically reviewed, timely revoked, and protected through facility security safeguards.
6	Controls are in place and operating effectively to ensure data center environmental and availability safeguards, including fire protection, environmental monitoring, backup power, and contingency planning, are maintained, monitored, updated, and tested to support continued operations.
7	Controls are in place and operating effectively to ensure changes and deployments impacting customer services are reviewed, tested, approved, validated, and monitored to support authorized and reliable implementation.

Superhuman Confidential
PROPIN - FOIA exempt

Attachment B – Principal Service Commitments and System Requirements

Superhuman designs its processes and procedures to support the product ecosystem in scope for this report, meeting objectives based on the following trust services criteria: security, availability, confidentiality, and privacy.

Those objectives are based on the service commitments that Superhuman makes to user entities; the laws and regulations that govern the provision of services; and the financial, operational, and compliance requirements that Superhuman has established for its control system.

Security, availability, confidentiality, and privacy commitments to user entities are described and communicated in detail in Superhuman's Terms of Service and Privacy Policy, as well as on its Trust landing page and User Trust Guidelines, all of which are available to end users and organization customers on Superhuman's public website. The Terms of Service and Privacy Policy are also described and communicated on Superhuman's sign-up page, browser extension stores, and through the iOS, Mac, and Android app stores. The same security, availability, confidentiality, and privacy commitments detailed in the Terms of Service and Privacy Policy are also outlined in the Master Service Agreements (MSAs) with enterprise customers.

The responsibilities of Superhuman are:

- Hosting and maintaining the Superhuman Platform System and associated services
- Reviewing and monitoring the Superhuman Platform System and associated services
- Technical support
- Process for customers to set up secure user accounts

The security, availability, confidentiality, and privacy commitments include, but are not limited to, the following:

- *Product Security* – Superhuman has a range of security controls designed to keep its systems secure, protect customers' data against unauthorized access, and guide necessary changes. These controls include, but are not limited to, implementing security processes and tools for change, vulnerability, and incident management to prevent, detect, and remediate security threats and vulnerabilities.
- *System Availability* – Superhuman monitors its systems' availability for customers by using cloud hosting across multiple availability zones in AWS regions, maintains optimal infrastructure performance through continuous monitoring, and establishes backups and Disaster Recovery Plans to enable quick, effective recovery in the event of an incident.
- *Data Security and Confidentiality* – Security and confidentiality controls at Superhuman are designed to meet the relevant criteria for protecting confidential information. Such controls include establishing and maintaining an information classification and service criticality procedure, business impact analysis (BIA) and risk assessment processes, proper access management, and encryption and other practices to restrict access to customers' data.

Superhuman Confidential
PROFIN - FOIA exempt

- *Privacy Process* – A range of privacy controls is designed to address the privacy criteria for Superhuman's product offerings and protect customers' personal information. Such privacy controls include maintaining a public Privacy Policy, providing a privacy notice to customers when there is a major change to the Privacy Policy, communicating publicly about Superhuman's sub-processors and any changes to them, providing timely responses to customer requests, and maintaining an established procedure to notify customers of breaches.

Superhuman Confidential
PROPIN - FOIA exempt