VENDASTA

Service Organization Control 3 (SOC 3®)

Vendasta Technologies Inc.'s report on its Yesware & Vendasta Platform relevant to Security for the period October 1, 2025 to March 31, 2026

mhm professional corporation
CHARTERED PROFESSIONAL ACCOUNTANT

Table of Contents

Section I **1**

Vendasta Technologies Inc.'s Management Assertion 2

Section II **4**

Independent Service Auditor's Report 5

Attachment A **8**

Vendasta Technologies Inc.'s Description of the Boundaries of its Yesware & Vendasta Platform 9

Digital Marketing and Business Services 10

AI Workforce Services 10

Service Delivery Model 11

White-Label Channel Partner Model 11

Infrastructure 11

Vendasta 11

Yesware 14

Network Architecture 16

Encryption 16

Endpoint Security 17

Software 18

Application Architecture 18

AI Models and Providers 18

Authentication and Authorization 19

Multi-Tenant Data Isolation 20

Monitoring and Observability 20

Security Tooling 21

Development Tools 22

People 23

Policies, Processes & Procedures 23

Data 25

Data Classification 26

Data Retention and Disposal 27

Attachment B **29**

Principal Service Commitments and System Requirements 30

Section I

Vendasta Technologies Inc.’s Management Assertion

Vendasta Technologies Inc.'s Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Vendasta Technologies Inc.'s ("Vendasta") Yesware & Vendasta Platform ("system") throughout the period October 1, 2025, to March 31, 2026, to provide reasonable assurance that Vendasta Technologies Inc.'s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Vendasta uses subservice organizations to provide cloud infrastructure services. The description of the boundaries of the system in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Vendasta, to achieve Vendasta's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Vendasta's controls. The description does not disclose the actual controls at the subservice organizations.

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 Vendasta Technologies Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("applicable trust services criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Vendasta Technologies 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.

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 Vendasta Technologies Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Dale Hopkins, CTO
Vendasta Technologies Inc.
July 15, 2026

Section II

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Vendasta Technologies Inc.:

Scope

We have examined Vendasta Technologies Inc.'s ("Vendasta") accompanying assertion titled "Vendasta Technologies Inc.'s Management Assertion" ("assertion") that the controls within the Vendasta Technologies Inc. Yesware & Vendasta Platform ("system") were effective throughout the period October 1, 2025 to March 31, 2026, to provide reasonable assurance that Vendasta Technologies Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Vendasta uses subservice organizations to provide cloud infrastructure services. The description of the boundaries of the system in Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Vendasta, to achieve Vendasta's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Vendasta's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

Service organization's responsibilities

Vendasta Technologies Inc. is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that Vendasta's service commitments and system requirements were achieved. In Section I, Vendasta has provided the accompanying assertion titled "Vendasta Technologies Inc.'s Management Assertion" ("assertion"), about

the effectiveness of controls within the system. When preparing its assertion, Vendasta Technologies 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.

Service auditors' responsibilities

Our responsibility is to express an opinion, based on our examination, on whether 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 the Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These 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.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Vendasta's service commitments and system requirements based on the applicable trust criteria.
- 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 achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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.

Opinion

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

Chartered Professional Accountant
Calgary, Alberta
July 15, 2026

Attachment A

Vendasta Technologies Inc.'s Description of the Boundaries of its Yesware & Vendasta Platform

VENDASTA

Vendasta Technologies Inc.'s Description of the Boundaries of its Yesware & Vendasta Platform

Company and Business Overview

Vendasta Technologies Inc. ("Vendasta" or "the Company") is a privately held technology company headquartered in Saskatoon, Saskatchewan, Canada. Founded in 2008, Vendasta has grown to over 600 employees operating from three offices: Saskatoon, Canada(headquarters), Boca Raton, Florida, and Chennai, India. Vendasta develops and operates a cloud-based, white-label software-as-a-service (SaaS) platform that enables channel partners – including digital agencies, managed service providers, media companies, and value-added resellers – to market, sell, bill, fulfill, and deliver digital solutions to small and medium-sized businesses (SMBs). The platform serves channel partners and their SMB clients worldwide.

Yesware provides sales enablement services for sales professionals in the United States and internationally. Yesware offers services that include team collaboration, e-mail tracking, custom templates, customer relationship management (CRM) system syncing, e-mail sequencing, meeting scheduling, reports, and analytic solutions. Yesware provides Pro, Premium, and Enterprise subscription plans that are tailored to fit everyone from individual professionals to large sales teams. Yesware was incorporated in 2010 and is headquartered in Boston, Massachusetts. On October 15, 2022, Yesware was acquired by Vendasta Technologies Inc., headquartered in Saskatoon, Saskatchewan, Canada. The organization retains some of the original staff who work remotely as Yesware no longer has a physical office in Boston, MA.

Services Provided

The Vendasta platform provides the following categories of services to its channel partners and their SMB clients:

Core Platform Services

Service	Description
CRM and Sales Intelligence	Customer relationship management with pipeline management, prospect analysis, campaign management, and order processing
Workflow Automation	Automated workflows for sales, marketing, fulfillment, and customer onboarding processes
Billing and	Integrated billing, invoicing, and payment processing for channel

Service	Description
Invoicing	partners and their SMB clients
Client Dashboard	White-labeled, single sign-on portal for SMB clients to manage their digital products and view analytics
Marketplace	Curated marketplace of digital solutions from third-party vendors available for channel partners to resell
AI Employee Platform	Platform for building, configuring, deploying, and managing AI employees and applications tailored to business needs

Digital Marketing and Business Services

Vendasta's Digital Marketing and Business Services is a professional services group that specializes in marketing and the customization and management of the Vendasta platform to the needs of customers.

AI Workforce Services

Service	Description
AI Receptionist	Automated inbound call handling, appointment scheduling, and caller routing
AI Reputation Specialist	Automated review monitoring and AI-generated review responses
AI Content Creator	AI-powered generation of blog posts, social media content, and email campaigns
Custom AI Employees	Business-specific workflow automation using AI agents

AI Workforce services utilize large language models and AI services provided by third-party AI service providers, including OpenAI, Anthropic, Google, ElevenLabs, and Deepgram, to process data and generate responses. These third-party AI providers are identified as subservice organizations.

Service Delivery Model

White-Label Channel Partner Model

Vendasta delivers its platform through a white-label channel partner model. Channel partners subscribe to the Vendasta platform and resell digital solutions to their SMB clients under the partner's own brand. In this model:

- Channel partners access the platform through a partner-branded administration portal where they manage their SMB client accounts, configure services, and monitor performance.
- SMB end users interact with the platform through partner-branded interfaces and may not be aware that Vendasta is the underlying platform provider.
- Vendasta operates and maintains the platform infrastructure, application logic, and data stores.
- Channel partners are responsible for managing their end-user relationships, configuring their white-label environments, and administering user access within their tenant.

The Boundaries of the System Used to Provide the Services

The boundaries of the system are the specific aspects of Vendasta Technologies Inc.'s infrastructure, software, people, procedures and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly supports the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as described in the sections below.

Infrastructure

Vendasta

All Vendasta platform services are hosted on Google Cloud Platform (GCP). Vendasta does not operate its own data centers. Physical data center security, environmental controls, and infrastructure-level network security are the responsibility of Google LLC.

GCP Services

The following GCP services are used in the delivery of the Vendasta platform:

GCP Service	Purpose	Relevance
Google Kubernetes Engine (GKE)	Container orchestration for platform microservices	Primary compute platform
Google App Engine	Application hosting for legacy microservices	Legacy compute platform
Cloud Run	Containers as a Service for highly dynamic workloads	Modern compute platform
Cloud Spanner	Globally distributed relational database	Primary datastore
Cloud Datastore	NoSQL document database	Legacy data storage
Cloud SQL	Managed relational database service	Relational data storage
Cloud Storage	Object storage for files, media, and backups	Data persistence
BigQuery	Data warehouse for analytics and reporting	Analytics and reporting
Pub/Sub	Asynchronous message queue for inter-service communication	Event-driven architecture
Cloud Task Queues	Task scheduling and execution with rate limiting	Rate limiting and deferred processing
Cloud Secret Manager	Secure storage of credentials, API keys, and certificates	Secret management
Cloud KMS	Encryption key management	Key management for data encryption
Cloud IAM	Identity and access management for GCP resources	Infrastructure access control

GCP Service	Purpose	Relevance
Cloud Logging	Centralized log aggregation	Audit trail and monitoring
Cloud Monitoring	Infrastructure and application metrics	Operational monitoring and alerting
Cloud Load Balancing	Traffic distribution and SSL termination	High availability and TLS termination
Cloud Armor	Web application firewall and DDoS protection	Application-layer security
VPC Networking	Virtual private cloud network isolation	Network segmentation

GCP Regions and Zones

All production workloads are deployed in the us-central1 region. The primary GKE cluster ("vendasta-central") runs in us-central1 as a regional cluster providing multi-zone resilience. Cloud Spanner instances, Cloud SQL instances, Cloud Run services, and App Engine services are also deployed in us-central1.

GCP Project Structure

Vendasta uses a multi-project GCP structure with separate projects for production and demo/development environments where feasible. The primary production project is repcore-prod, which hosts the main platform infrastructure including:

- The "vendasta-central" GKE cluster (production and demo workloads isolated via separate node pools and namespaces)
- Cloud Spanner instances Cloud SQL instances App Engine services
- Approximately 270 Cloud Run services (production and demo)

Additional platform services are deployed in dedicated per-service GCP projects following a consistent naming convention (e.g., service-prod / service-demo), providing project-level isolation between services.

Yesware

At the infrastructure and platform layers, the Yesware Platform's compute is hosted on the Amazon Web Services (AWS) Elastic Kubernetes Service (EKS). This compute is supported by a number of managed databases and queuing systems including:

- Cloud AMQP (hosted RabbitMQ) for queuing
- Redis Labs managed database for caching
- MongoDB Atlas databases
- Google Cloud SQL databases
- Heroku's managed Kafka solution for stream processing
- Twilio's Segment for user-behaviour processing pipelines
- Twilio's SendGrid for transactional emails

Additionally, Yesware leverages a number of hosted tools for data warehousing:

- Google Looker for reporting
- Google BigQuery for Data Warehousing & Reporting
- Snowflake for Data Warehousing & Reporting

Each of the above services is hosted within the boundaries of either AWS or Google Cloud Platform (GCP).

A summary of the technology used to support the Yesware Platform is as follows:

- A SailPoint directory service application used to manage access to corporate resources.
- Google Workspace is used for team collaboration and communication
- Jira ticketing system is utilized to track and solve issues and plan changes
- Confluence wiki is utilized to collaborate system changes and build automation.
- Terraform and Helm are utilized to automate configuration and internal technology (IT) infrastructure.

An overview of the authentication process is as follows:

- Corporate password management provides scoped access to micro-applications and cloud platforms that do not support Google Single Sign-On
- Google Single Sign-On (SSO) implemented to manage role-based access to Yesware infrastructure, as well as manage access to additional cloud-based company resources.

The in-scope infrastructure consists of multiple systems, platforms, and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Yesware Extension	Plugin for Gmail, Outlook365, and Outlook web application	Google Chrome / Microsoft Office Add-in	AWS (US East)
Yesware Applications	Suite of Yesware applications	AWS EKS	
Kafka	Event streaming platform, storage for event data & metadata	Heroku Platform	
RabbitMQ	Message Queues, Storage	Cloud AMQP IaaS	
Snowflake	Data Warehouse	Snowflake IaaS	
MongoDB	Database, storage for metadata, backups	MongoDB Atlas IaaS	GCP (US-east)
Redis		Redis Labs IaaS	
PostgreSQL	Database storage for metadata, backups	Google Cloud SQL	
Looker	Reporting	Google Looker	GCP (US)

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Big Query	Data Warehouse	Google BigQuery	

Network Architecture

The production environment in repcore-prod uses multiple VPC networks for network segmentation, including dedicated networks for services requiring static egress and isolated workloads. The environment is protected by 109 firewall rules governing traffic flow between network segments.

- **VPC configuration:** Multiple VPC networks provide segmentation between production workloads, with dedicated networks for specific service tiers.
- **Firewall rules:** Firewall rulesets are reviewed at least annually, and required changes are tracked to completion.
- **Load balancing:** GCP Cloud Load Balancing distributes traffic and handles SSL/TLS termination for customer-facing endpoints.
- **Edge security:** Cloudflare provides CDN, DNS management, WAF, and DDoS protection at the edge layer.
- **Internal communication:** Services communicate within the GKE cluster and across Cloud Run services via internal networking.
- **External access:** External-facing APIs are protected by Cloudflare and GCP Cloud Armor.

Encryption

Data State	Encryption Standard	Key Management
Data at rest	AES-256	Google-managed encryption keys (GMEK) — encryption at rest is handled automatically by GCP for all data services
Data in transit (external)	TLS 1.2 or higher	Managed TLS certificates for customer-facing endpoints via

Data State	Encryption Standard	Key Management
		Cloudflare and GCP Cloud Load Balancing
Data in transit (internal)	mTLS (mutual TLS)	Services authenticate each other via mutual TLS certificates for inter-service communication
Data in transit (to subservice orgs)	TLS 1.2 or higher	Provider-managed certificates
Backups	AES-256	Encrypted at rest using Google-managed keys (same standard as primary data)

Encryption key access is restricted to authorized users with a business need (control CRY-2). Key management is handled by Google as part of the GMEK model, with Google managing key rotation automatically.

Endpoint Security

Corporate devices used by Vendasta employees to access production systems are managed through:

- **Mobile device management (MDM):** MDM is used to centrally manage corporate devices, enforce security policies, and maintain device inventory.
- **Endpoint detection and response (EDR):** Anti-malware technology is deployed on all corporate endpoints, configured for routine updates and centralized logging.
- **Disk encryption:** Full disk encryption is required on all corporate devices.
- **OS and software patching:** Patching requirements are enforced through MDM policies.
- **Remote access:** Production systems can only be remotely accessed by authorized employees via approved encrypted connections with multi-factor authentication.

Software

Application Architecture

The Vendasta platform is built on a microservices architecture deployed across three compute platforms. The platform comprises approximately 270 Cloud Run services, services deployed on the "vendasta-central" GKE cluster, and legacy services on App Engine. Services communicate primarily via gRPC for synchronous calls and Pub/Sub for asynchronous messaging.

Key architectural components include:

Component	Technology	Purpose
Legacy application hosting	Google App Engine	Legacy microservice hosting
Modern container hosting	Google Cloud Run (~270 services)	Containers as a Service for highly dynamic workloads
Synchronous communication	gRPC	Inter-service request/response
Asynchronous messaging	Google Cloud Pub/Sub	Event-driven workflows, decoupled service communication
Workflow orchestration	Temporal Cloud (hosted)	Long-running business process automation
Search	Elasticsearch (dedicated GKE clusters)	Full-text search and indexing
Caching	RedisLabs / GCP Memorystore	Performance optimization and caching
Primary datastore	Cloud Spanner (3 instances)	Globally distributed relational database
Relational databases	Cloud SQL (MySQL, PostgreSQL)	Service-specific relational data storage

AI Models and Providers

The Vendasta platform integrates with multiple third-party AI model providers to power AI Workforce and AI Employee Platform features. The platform's AI orchestration layer abstracts provider-specific APIs and manages model selection, data routing, and response handling.

Provider	Services	Platform Features Powered	Data Handling
Google (Vertex AI)	Various LLM and ML models	AI Workforce and AI Employee Platform features	Per GCP data processing agreement
Anthropic	Various Claude models	AI Workforce and AI Employee Platform features	Per Anthropic API data usage policy
OpenAI	Various GPT models	AI Workforce and AI Employee Platform features	Per OpenAI API data usage policy
ElevenLabs	Text-to-speech models	AI voice synthesis for AI Workforce features	Per ElevenLabs API terms
Deepgram	Speech-to-text models	Audio transcription for AI Workforce features	Per Deepgram API terms

All AI provider integrations are configured to transmit data via authenticated, encrypted API calls (TLS 1.2+). These third-party AI providers are identified as subservice organizations in this description.

Authentication and Authorization

The platform's identity and access management (IAM) system provides authentication and authorization for all platform users, including Vendasta employees, channel partners, and SMB end users.

Authentication: - User authentication is performed securely via the IAM service. - Single sign-on (SSO) through trusted identity providers (e.g., Google, Microsoft) is the preferred authentication method. - Passwords are stored as salted hashes with enforced minimum complexity requirements. - Multi-factor authentication (MFA) is delegated to third-party SSO providers (Google, Microsoft). Vendasta does not currently implement MFA natively

within the platform. The result of successful authentication is the return of a JWT-bearer token for session management.

Authorization: - The IAM system implements policy-based access control where access decisions are evaluated against resource ownership and subject attributes. - Caller identity is propagated across the service mesh via JWT sessions and custom headers, enabling each service to validate tenant context and enforce access policies. - Access policies are defined in a version-controlled repository and deployed through the standard CI/CD pipeline, providing change management controls over authorization rules.

Multi-Tenant Data Isolation

The Vendasta platform is a multi-tenant system serving multiple channel partners and their SMB clients. Tenant isolation is enforced at three architectural layers:

Layer 1 – Database/Storage Layer: Customer data is logically segregated using namespace isolation. Each tenant's data is isolated within separate namespaces in the shared database infrastructure, ensuring that database operations are scoped to the appropriate tenant context.

Layer 2 – Service/API Layer: All API requests are authenticated and include tenant context derived from the authenticated session. The platform's IAM interceptors propagate tenant context across the service mesh, validating authorization on every inter-service call. Tenant context is propagated through request headers and validated at each service boundary, preventing cross-tenant data access at the API layer.

Layer 3 – Application/UI Layer: Each channel partner accesses the platform through a dedicated, white-labeled instance configured with their branding and domain. The application session is bound to the partner's tenant context, and all data rendered in the UI is filtered by the authenticated tenant identifier.

Monitoring and Observability

Function	Tool	Description
Infrastructure monitoring	GCP Cloud Monitoring	Infrastructure metrics, resource utilization, and automated alerting on predefined thresholds
Application performance	Datadog	APM, distributed traces, custom metrics, and application-level monitoring

Function	Tool	Description
Log aggregation	GCP Cloud Logging / Datadog	Centralized log collection with defined retention periods
Alerting and on-call	PagerDuty	Incident alerting, escalation tiers, and on-call rotation management
Error tracking	Sentry	Application error tracking and real-time alerting
Uptime monitoring	Datadog	Automated health checks and synthetic transactions
Security monitoring	Datadog Security	Security event detection and monitoring with configured detection rules
Compliance monitoring	Vanta	Continuous monitoring of SOC 2 controls and automated evidence collection

Security Tooling

Function	Tool	Description
CDN / WAF / DDoS protection	Cloudflare	Edge security, web application firewall, and DDoS protection
Cloud WAF	GCP Cloud Armor	Application-layer security for GCP-hosted endpoints
Vulnerability scanning	grype	Build artifact scanning run on every build.
Vulnerability disclosure	HackerOne	Bug bounty and vulnerability disclosure program (active since July 2020)

Function	Tool	Description
Endpoint protection / MDM	JumpCloud	MDM, endpoint security policy enforcement, and centralized device management
Secret management	GCP Cloud Secret Manager	Secure storage of credentials, API keys, and certificates
Compliance automation	Vanta	Continuous control monitoring, evidence collection, and SOC 2 readiness tracking
Background checks	Checkr	Automated background check processing for new hires

Development Tools

Function	Tool	Description
Version control	GitHub	Source code management with branch protection and access controls
CI/CD pipeline	Google Cloud Build	Automated build, test, and deployment
Code review	GitHub Pull Requests	Peer review and approval are required before merging to the master branch
Deployment	Mission Control (internal tool)	Production deployment orchestration
Project management	Jira	Issue tracking, sprint management, and change request documentation
Documentation	Confluence	Technical documentation and collaboration on system changes
Knowledge management	Guru	Internal knowledge base for operational procedures
Customer support	Zendesk	External-facing support system for incident and issue reporting

People

Organizational Structure

Vendasta employs over 600 personnel across three offices. *Functional Groups*

- **Product Management and Support** – responsible for product strategy, roadmap, and customer support.
- **Engineering and Engineering Operations** – develops, manages, and operates the core software and services, oversees vendor-managed infrastructure as well as services deployed on GCP.
- **Customer Success** – responsible for overall customer relationships, strategic account management, and customer solutions.
- **Marketing** – performs marketing and business development functions.
- **General and Administrative (G&A) / Finance** – performs financial management and accounting functions, office management, human resources, and recruiting.
- **Information Security** – oversees security and compliance activities for the company and the company's products.

The teams and associated initiatives, workstreams, and functions are led by the executive management leads.

Policies, Processes & Procedures

Vendasta maintains security policies and procedures covering information security, acceptable use, access control, change management, incident response, business continuity and disaster recovery, vendor management, data classification, data retention and disposal, code of conduct and ethics, whistleblower protections, human resources security, vulnerability management, network and system hardening standards, and the secure software development lifecycle. These policies are documented, reviewed at least annually, and made available to all employees. Critical policies must be read and accepted before beginning job functions.

The following policies and procedures are available to employees and contractors through the Vanta Platform:

- Access Control Policy: Limits access to systems, networks, and facilities to authorized parties.

- Asset Management Policy: Identifies organizational assets and defines protection responsibilities.
- Business Continuity and Disaster Recovery Plan: Prepares for extended outages to restore services quickly. (Draft version available)
- Code of Conduct: Maintains a standard of conduct for employees, customers, and vendors. (Draft version available)
- Cryptography Policy: Ensures effective use of cryptography to protect information integrity.
- Customer Privacy Policy: Privacy policy specifically for Vendasta customers.
- Data Management Policy: Covers classification, protection, and secure disposal of information.
- Human Resource Security Policy: Ensures personnel meet security requirements and understand their roles.
- Incident Response Plan: Establishes the plan for managing and responding to security incidents.
- Information Security Policy (AUP): Outlines acceptable use and protection of information and assets.
- Information Security Roles and Responsibilities: Establishes critical roles for policy communication and standards.
- Learning and Development Framework: Requires security awareness training for all employees.
- Operations Security Policy: Ensures secure operation of processing systems and facilities.
- Physical Security Policy: Prevents unauthorized physical access to facilities.
- Risk Management Policy: Defines the methodology for assessing and managing security risks.
- Secure Development Policy: Ensures security is designed into the application development lifecycle.

- Third-Party Management Policy: Manages security for data and assets shared with external suppliers.

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. Vendasta has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

The Vendasta platform processes the following categories of data:

Data Category	Description	Examples
Partner account data	Information about channel partner organizations and their administrators	Company name, admin email, contact info, billing details
SMB business data	Information about small businesses managed through the platform	Business name, address, phone, website, hours, categories
End consumer data	Information about the SMB's customers or contacts	Names, email addresses, phone numbers, interaction history
Review and reputation data	Customer reviews and ratings aggregated from third-party sources	Review text, ratings, reviewer names, source platform
Content data	Marketing content created through or managed by the platform	Blog posts, social media posts, email campaigns, ad copy

Data Category	Description	Examples
AI & CRM interaction data	Data processed by AI Workforce features and data in the CRM.	Call transcripts, AI-generated responses, prompt/completion logs, sales activities, customer messages & interactions
Billing and financial data	Payment and billing information	Invoicing data, subscription details, payment tokens. Credit card processing is delegated to Stripe (Vendasta platform) and Worldpay (Yesware direct customers); Vendasta does not store credit card numbers
Authentication credentials	User login credentials	Passwords (stored as salted hashes), session tokens, API keys
Platform usage data	Analytics and telemetry about platform usage	Feature usage metrics, performance data, error logs

Data Classification

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel

Classification Level	Description	Examples	Handling Requirements
Confidential	Data that requires protection and is restricted to authorized personnel	Customer data, authentication credentials, API keys, billing data, AI interaction data	Encrypted at rest and in transit; access restricted to authorized personnel with a business need; logged access
Public	Data that is intentionally made available to the public	Marketing materials, published help documentation, public API documentation	No special handling requirements

Data Retention and Disposal

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. The company has a standard operating procedure for handling Data Deletion Requests.

Data Type	Retention Period	Disposal Method
Active customer data	Duration of service agreement	N/A — active data
Terminated customer data	Retained until customer requests deletion	Secure deletion in accordance with Data Deletion Request SOP
Backup data	Per backup retention schedule	Automated expiry
Audit logs	Per log retention policy	Automated expiry
AI interaction logs	Per log retention policy	Automated expiry
Electronic media	N/A	Purged or destroyed with certificates of destruction issued per device

When a partner churns or an SMB is offboarded, customer data is retained until a formal Data Deletion Request is received. Upon receipt, data is purged in accordance with the company's Data Deletion Request Standard Operating Procedure.

Data is entered via the Angular client web application and sent to the application servers via REST calls to the API. The data is processed and written to the Google Cloud Datastore instance. Data transmission is secured using TLS 1.2 with PKCS #1 v2.2, SHA-512 hashing, and RSA encryption, and does not leave the VPC. Data replication channels are also encrypted and remain internal to Google Cloud, moving only within the private VPC. All data access requests require an ACL context which contains both the authenticated user and the organization that is requesting the data. These requests are

validated via the Vendasta permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using AES-256 encryption.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Security Commitments

Security commitments to user entities are documented and communicated in the terms of service and security webpage. The principal security commitments are standardized and include, but are not limited to, the following:

- maintaining administrative and technical safeguards to protect the security of information provided to Vendasta;
- performing web activity over a secure transport layer security (TLS) connection;
- utilizing strong passwords and multi-factor authentication for Vendasta employee access to production systems, and providing multi-factor authentication capabilities to channel partners for access to the platform;
- monitoring of systems for performance management and vulnerabilities; and
- notifying users of a security breach with steps to minimize damages.

Vendasta establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Including the use of encryption technologies to protect data in transit; enforcing multi-factor authentication paired with a strong password policy, utilizing logging and monitoring tools for security incidents and vulnerability assessments, and having documented escalation policies and procedures.

Such requirements are communicated on Vendasta's website. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Vendasta platform.

Note that there may be service commitments made to individual users that fall outside of the specifications above and as such are not covered in this document.

Availability Commitments

Availability is not contractually committed to channel partners through SLAs or uptime guarantees. While Vendasta maintains operational practices to support platform reliability, no formal availability commitments are made in customer-facing agreements. The Availability trust services category is not in scope for this examination.