System and Organization Controls (SOC) 3

Report on Eleven Labs, Inc.'s AI-powered Audio and Voice Generation System Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy Throughout the Period July 1, 2025, to June 30, 2026

IIElevenLabs

INSIGHT ASSURANCE

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT 1

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION 2

SECTION 2: ELEVEN LABS, INC.'S MANAGEMENT ASSERTION 4

ELEVEN LABS, INC.'S MANAGEMENT ASSERTION 5

ATTACHMENT A: DESCRIPTION OF THE SYSTEM BOUNDARIES 6

ELEVEN LABS, INC.'S DESCRIPTION OF THE BOUNDARIES OF THE AI-POWERED AUDIO AND VOICE GENERATION SYSTEM 7

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 14

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 15

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION

To: Eleven Labs, Inc.

Scope

We have examined Eleven Labs, Inc.'s ("ElevenLabs") accompanying assertion titled "Eleven Labs, Inc.'s Management Assertion" (assertion) that the controls within the AI-powered Audio and Voice Generation System (system) were effective throughout the period July 1, 2025, to June 30, 2026, to provide reasonable assurance that ElevenLabs' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, 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*.

Service Organization's Responsibilities

ElevenLabs 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 ElevenLabs' service commitments and system requirements were achieved. ElevenLabs has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ElevenLabs 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 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 American Institute of Certified Public Accountants. 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 ElevenLabs' 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 ElevenLabs' 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.

Opinion

In our opinion, management's assertion that the controls within the AI-powered Audio and Voice Generation System were effective throughout the period July 1, 2025, to June 30, 2026, to provide reasonable assurance that ElevenLabs' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
September 29, 2026

SECTION 2:
ELEVEN LABS, INC.'S MANAGEMENT ASSERTION

IIElevenLabs

ELEVEN LABS, INC.'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Eleven Labs, Inc.'s ("ElevenLabs") AI-powered Audio and Voice Generation System throughout the period July 1, 2025, to June 30, 2026, to provide reasonable assurance that ElevenLabs' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, 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 July 1, 2025, to June 30, 2026, to provide reasonable assurance that Eleven Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. Eleven Labs, 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 July 1, 2025, to June 30, 2026, to provide reasonable assurance that Eleven Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Eleven Labs, Inc.
September 29, 2026

ATTACHMENT A:
DESCRIPTION OF THE SYSTEM BOUNDARIES

ATTACHMENT A

ELEVEN LABS, INC.'S DESCRIPTION OF THE BOUNDARIES OF THE AI-POWERED AUDIO AND VOICE GENERATION SYSTEM

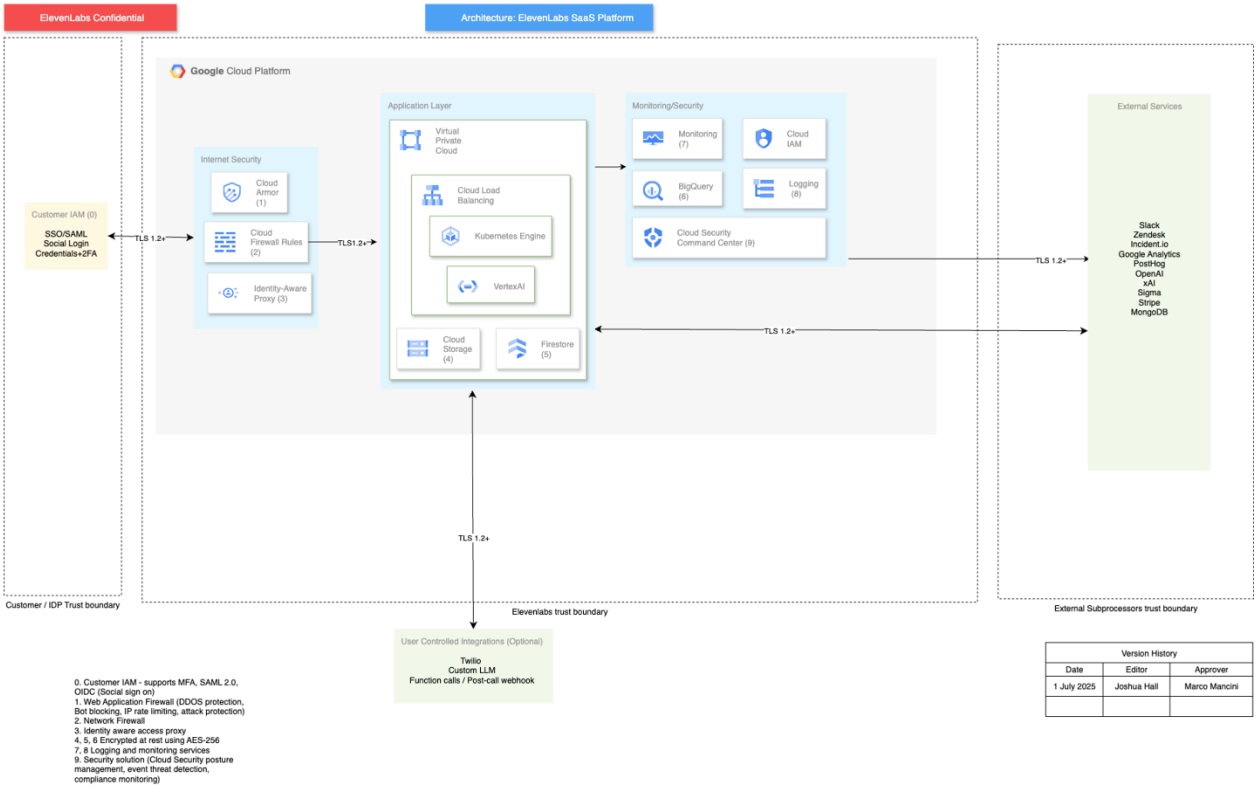
SERVICES PROVIDED

The speech services provide a platform to transform written text into high quality AI generated audio, create and clone voices, and transform existing speech for example from one voice and/or language to another voice and/or language. The service supports multiple languages, ensuring global reach, scalability, and reliable performance. With advanced algorithms and customizable features, clients can enhance accessibility, personalize user experiences, and save time and resources. ElevenLabs prioritizes data privacy and security while maintaining regulatory compliance. The System is delivered from a default multi-tenant environment hosted in the United States. For enterprise customers with data residency requirements, ElevenLabs operates additional regional environments that deliver the same services from infrastructure located in the selected region. For enterprise customers processing sensitive content, ElevenLabs offers Zero Retention Mode (ZRM) on eligible API services. When ZRM is enabled, request inputs and generated outputs are processed in memory and are not written to persistent storage or logs after the request completes.

INFRASTRUCTURE

ElevenLabs maintains a system inventory that includes virtual machines (Google Compute Engine) and endpoints (laptops). The inventory documents device name, device type, vendor function, OS, location, and notes. The system includes the whole AI-powered Audio and Voice Generation System Platform, including the default SaaS environment and any additional data residency locations that may be deployed by ElevenLabs from time to time.

To outline the topology of its network, the organization maintains the following network diagram:



The ElevenLabs application infrastructure is located primarily at Google Cloud Platform (GCP) data centers, with additional compute capacity for model inference workloads hosted at Amazon Web Services (AWS). AWS and GCP act as hosting subservice organizations for the company. The subservice organizations provide physical security and environmental protection controls, as well as managed services for ElevenLabs' infrastructure. The AWS environment connects to the GCP production network over redundant IPsec VPN tunnels with BGP routing and is managed under the same infrastructure-as-code, access control, logging, and vulnerability management processes as the GCP environment.

GCP's network security uses hardware- and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

Deployment Regions and Data Residency

The default environment is hosted in GCP's United States region. Regional data residency environments are deployed as dedicated sets of GCP projects in the selected region, each with its own network, storage, and database resources, with data encrypted at rest, so that customer content is stored and processed within that region. During the examination period, residency environments were operated in the European Union and India. All regional environments are provisioned from the same infrastructure-as-code repository and are subject to the same policies, controls, monitoring, and change management processes described in this report.

In addition to the firewall, ElevenLabs uses anti-virus and anti-spyware applications to protect systems from viruses.

ElevenLabs' Information Security Policy and security procedures ensure that all computer devices have available virus protection software, and the most recent operating system and security patches installed.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize security mechanisms inherent to the Google Cloud container-optimized Operating System. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on ElevenLabs-owned computers; they may install software only in accordance with company's acceptable use policy, which is regularly reviewed and maintained by the CTO.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Google Cloud Armor	Security Service	Web Access Firewall services and Anti-DDoS protection
GCP VPC	Network Service	Virtual Private Cloud for secure and scalable network infrastructure
Kubernetes Engine	Orchestration	Container orchestration and management
Cloud Load Balancing	Cloud Service	Distributing incoming traffic across multiple resources for high availability
Firestore	Database Service	NoSQL database for real-time data synchronization and storage
Google Intrusion Detection System	Security Service	Monitoring network and systems for malicious activity
Google Cloud Storage	Storage Service	Object storage for scalable and secure data storage
Google Cloud Firewall	Security Service	Enforcing network security rules to control inbound and outbound traffic
BigQuery	Analytics Service	Data warehousing and analytics for large-scale data processing
MongoDB Atlas	Database Service	Managed document database for application data. It operated on GCP environment.
AWS VPC	Network Service	Isolated network for AWS-hosted workloads
AWS Site-to-Site VPN	Network Service	Encrypted connectivity between the AWS and GCP production environments
Amazon Elastic Kubernetes Service (EKS)	Orchestration	Container orchestration for workloads hosted in AWS

SOFTWARE

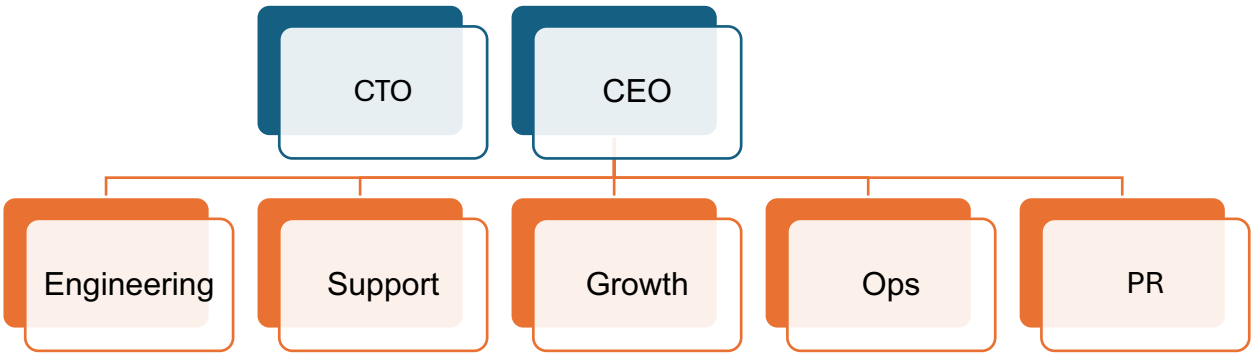
ElevenLabs maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

Primary Software	
System/Application	**Purpose**
GitHub	Code Management
Google Workspace	Identity management and authentication, Email, collaboration, and directory services
Terraform	Infrastructure and access provisioning as code
Wiz	Vulnerability scan
Vanta	Compliance management tool
Okta	Single sign-on and multi-factor authentication
SentinelOne	Endpoint detection and response
Google SecOps	Security logging and monitoring
Jamf Pro	Mobile device management

PEOPLE

The ElevenLabs staff provides support to the above services. ElevenLabs employs dedicated team members to handle all major product functions, including operations and support. The engineering team monitors the environment and manages data backups and recovery. The company focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep ElevenLabs and its data secure.

ElevenLabs' corporate structure includes the following roles:



Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Chief Technology Officer (CTO) – Responsible for the technological direction and advancements of the organization. Directs the engineering and research to efficiently create/present new services and maintain existing ones.

Security and Compliance – Responsible for the information security and compliance program, including policy ownership, risk assessment, control monitoring, audit coordination, and security incident coordination. Reports to executive management and provides regular updates on the security posture of the organization.

Operations (Ops) – Primarily responsible for daily aspects of internal business operations as well as temporary surges based on business needs.

Growth – Responsible for outreach to prospective clients and completing sales, which is also responsible for the maintenance and renewals of existing customer contracts. In addition, responsible for identifying and implementing optimization strategies to increase the reach of the customer base.

Public Relations (PR) – Responsible for the external communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of ElevenLabs.

Engineering – Responsible for software development, deployment and maintenance, as well as for the research and development of underlying models and new services.

Support – This role includes the support team and includes but is not limited to the support of end-users with day-to-day issues.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by ElevenLabs in delivering its services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees of ElevenLabs are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to ElevenLabs' business and finances are, as a matter of ElevenLabs policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Customer Success and Engineering Departments. Engineering is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

ElevenLabs has policies and procedures in place to ensure proper retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. For enterprise customers,

Customer Content is deleted within 30 days of expiration or termination of the customer agreement, in accordance with the Data Processing Addendum, and residual copies in backups expire within a further 30 days. Deletion is performed by the Engineering team.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications.	• Press releases • Public website
Internal	Non-sensitive information originating within or owned by ElevenLabs, or entrusted to it by others. Internal information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.	• Internal memos • Design documents • Product specifications • Correspondences
Confidential	Sensitive information that must be limited to only authorized employees, contractors, and business partners with a specific business need.	• Design documents • Product specifications • Research

Data		
Category	**Description**	**Examples**
Restricted	Highly sensitive information, where the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.	• Protected Health Information (PHI/ePHI) processed under an executed Business Associate Agreement • Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer

Zero Retention Mode.

Zero Retention Mode is enabled by ElevenLabs at the workspace level for enterprise customers upon request, and may also be enabled by the customer for individual ElevenAgents agents. In this mode, text and audio inputs, generated outputs, and the requesting user's email address are excluded from request history, databases, and backend logs. ZRM applies to API traffic only; requests made through the web application are retained in accordance with the customer's workspace retention settings. Under the ElevenLabs Business Associate Agreement, HIPAA-eligible services are Covered Services only while Zero Retention Mode is enabled, and ElevenLabs enables ZRM on the workspace as part of BAA execution.

PROCEDURES

Management has developed and communicated policies and procedures involved in the operation of the system. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business at least annually. The following provides a summary of ElevenLabs' policies and procedures that comprise the internal control for the system.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ElevenLabs designs its processes and procedures related to the ElevenLabs' Audio Services ("System") to meet its objectives. Those objectives are based on the service commitments that ElevenLabs makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that ElevenLabs has established for the services.

Security Commitments

Security commitments to user entities are documented and communicated in the Terms of Service, customer agreements, and the Trust Center at compliance.elevenlabs.io.

Security commitments are standardized and include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Continuous vulnerability scans over the system and network, and annual penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal.

ElevenLabs establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. 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 and trained.

In addition, the policies address how to carry out specific manual and automated processes required in the operation and development of the System.

Availability Commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Operational procedures supporting the achievement of availability commitments to user entities.

Processing Integrity Commitments

Processing Integrity commitments include, but are not limited to, the following:

- Controls exist to prevent or detect and correct processing errors to meet the entity's processing integrity commitments and system requirements.
- System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
- Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.
- Data is stored and maintained completely, accurately, and promptly for its specified life span to meet the entity's processing integrity commitments and system requirements.
- System output is complete, accurate, and distributed to meet the entity's processing integrity commitments and system requirements.
- Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.

Confidentiality Commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between ElevenLabs and user entities.
- Availability of Zero Retention Mode for eligible enterprise API services, under which customer inputs and outputs are not retained after processing.

Privacy Commitments

Privacy commitments include, but are not limited to, the following:

- The company defines documents, communicates, and assigns accountability for its privacy processes and procedures.
- The company provides notice about its privacy processes and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- The company describes the choices available to the individual and obtains implicit or explicit consent concerning the collection, use, and disclosure of personal information.
- The company collects personal information only for the purposes identified in the notice.
- The company limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
- The company discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

- The company protects personal information against unauthorized access (both physical and logical).
- The company maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- The company monitors compliance with its privacy policies and practices.