Identity Management Platform
Solution & Identity platform

System and Organization Controls 3 (SOC 3)
Report on the VERIDAS.
Relevant to Security, Availability, Confidentiality, and Privacy.

For the period from January 1, 2024, to December 31, 2024.

CONTENT

INDEPENDENT SERVICE AUDITOR'S REPORT 3

1. Scope 3
2. Responsibilities of the service organization 3
3. Responsibilities of the Service Auditor 3
4. Limitations of controls in a service organisation 5
5. Opinion 5
6. Description of the control tests 5
7. Targeted users and purpose 5

WRITTEN MANAGEMENT STATEMENT ON SERVICE ORGANIZATION 7

ATTACHMENT A- SYSTEM DESCRIPTION 9

SCOPE 9

RELEVANT ASPECTS OF GENERAL CONTROL 10

1.1 Control environment 11

1.2 Risk Assessment 11

1.3 Information and Communication 11

1.4 Control Activities 12

1.5 Monitoring and Internal Auditing 12

ATTACHMENT B- DETAILED DESCRIPTION OF THE CONTROL ENVIRONMENT 13

ATTACHMENT C- PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 21

INDEPENDENT SERVICE AUDITOR'S REPORT

To: VERIDAS Service Organization

1. Scope

We have been hired to report on the description made by the VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, of its Digital identity verification service, covering the activities of design, development, deployment, maintenance, enhancement, integration, support and marketing of software products for this service and Identity platform, during the period from January 1 2024 to December 31, 2024 (defined in Section III, System description), and on the design and effective operation of the controls related to the control objectives indicated in the description, to provide reasonable assurance that service commitments and system requirements were met based on trusted service criteria relevant to security and availability (capacity, processing integrity, confidentiality, and privacy).

2. Responsibilities of the service organization

The VERIDAS service organization is responsible: for the preparation of the description and the statement attached thereto (shown in section II of the report), as well as for the completeness, accuracy and method of presentation of the description and affirmation; to provide the services covered by the alert, to indicate the control objectives; to design, implement and effectively apply controls to achieve the stated control objectives; and select the applicable trust service criteria and establish the related controls in the Description; and identify risks that threaten the fulfillment of service commitments and system requirements of the Service Organization.

3. Responsibilities of the Service Auditor

Our responsibility is to express an opinion on the VERIDAS service organization's description and on the design and operation of controls relevant to the control objectives indicated in that description, based on our procedures. We conducted our order in accordance with International Standard on Assurance Engagements (ISAE) 3402 "Reports Providing Assurance on Controls in a Service Organization" issued by the International Standards on Auditing and Assurance Engagements Board. This standard requires us to follow ethical requirements and to plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and controls are properly designed and operating effectively, and Assurance Assignment Standard 3000: Assurance Assignments other than auditing or reviewing historical financial information, International Framework for Assurance Assignments and the concordance modifications of other

International Standards for Assurance Assignments-NIEA.

These standards require that we comply with ethical requirements and that we plan and implement our procedures in order to obtain reasonable assurance that, in all material respects, the description is presented faithfully and the controls are properly designed and function effectively.

An assignment that provides a degree of assurance about the description, design, and operational effectiveness of controls in a service organization involves the application of procedures to obtain evidence about the information disclosed in the service organization's description of its system, and about the design and operational effectiveness of controls.

The procedures selected depend on the judgment of the service auditor, as well as an assessment of the risks that the description is not presented faithfully and that the controls are not properly designed or are not working effectively. Our procedures included testing the operating effectiveness of controls we considered necessary to provide reasonable assurance that the control objectives indicated in the description were achieved. A security engagement of this type also includes assessment of the overall presentation of the description, the adequacy of the objectives stated in the description, and the adequacy of the criteria detailed by the service organization and described in Section III.

Believe that the evidence we have obtained provides a sufficient and adequate basis for our opinion.

Examination of a description of a service organization's system and the adequacy of the design and operational effectiveness of controls involves:

- Perform procedures to obtain evidence on the impartiality of the presentation of the Description and the suitability of the design and the operational effectiveness of the controls to achieve the related control objectives set out in the Description, based on the criterion in the management affirmation.
- Assess the risks that the Description is not presented adequately and that controls were not designed or functioned effectively to achieve the related control objectives set out in the Description.
- Test the operational effectiveness of such controls as management deems necessary to provide reasonable assurance that the related control objectives set out in the Description were achieved.
- Evaluate the overall presentation of the Description, the suitability of the control objectives established therein, and the suitability of the criteria specified by the service organization in its affirmation.

4. Limitations of controls in a service organisation

The description made by the VERIDAS service organization is prepared to meet the needs of its customers and auditors and it is possible, therefore, that it does not include every aspect of the system that your client may consider important in their particular environment. Likewise, due to their nature, it may happen that controls in a service organization do not prevent or detect all errors or omissions in the processing of transactions or in the preparation of reports on them. In addition, the forward-looking projection of any conclusions about the suitability of the design or the operational effectiveness of the controls is subject to the risk that the controls will become inadequate due to changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

5. Opinion

Our opinion has been formed on the basis of the issues mentioned in this report. The criteria we use in reaching our opinion are those described in Section IV.
In our opinion, in all material aspects:

*(a) The description faithfully presents the "*Digital identity verification service, covering the activities of design, development, deployment, maintenance, enhancement, integration, support and marketing of software products for this service and Identity platform*" as designed and implemented during the period from* January 1 2024 to December 31, 2024*;*
(b) The controls related to the control objectives referred to in the description were properly designed during the period from January 1 2024 to December 31, 2024 *;and*
(c) The controls that were tested, which were those necessary to provide reasonable assurance that the control objectives indicated in the description were achieved, functioned effectively during the period from January 1 2024 to December 31, 2024.

6. Description of the control tests

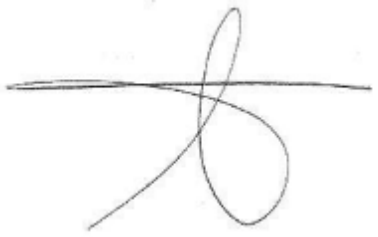
The specific controls that were tested and the nature, timing and results of such tests are detailed in Section IV of this report.

7. Targeted users and purpose

This report and the description of the Section IV control tests are intended only for clients who have used VERIDAS' Digital identity verification service, and for its auditors, who have sufficient knowledge to take them into account, together with other information, including information on the controls applied by clients themselves, in assessing the risks of material

misstatement in customers' financial statements.

ingertec
B84534965
Avda. Torrecilla s/n
Centro Industrial La Torre, Parc.38, Nave 38
14013 Córdoba



WRITTEN MANAGEMENT STATEMENT ON SERVICE ORGANIZATION

We have prepared the description of the VERIDAS system (the "service organization") related to the characteristics of the Digital identity verification service and Identity Platform (the "Description"), for customers who have used the VERIDAS Digital identity verification service during the period from January 1 2024 to December 31, 2024.

The description includes only the control objectives and related controls of VERIDAS and excludes the control objectives and related controls of the subservice organization.

The description indicates that certain control objectives specified in the description can only be achieved if the complementary user entity controls assumed in the design of the VERIDAS controls are properly designed and functioning effectively, together with those related to the controls in the service organization. The description does not extend to the controls of the user entities.

The description is intended to provide reporting users with information about our system that may be useful in assessing the risks arising from interactions with the VERIDAS system, in particular information about the system controls that VERIDAS has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria of trust relevant to security and availability.

Criteria description

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents the VERIDAS system that was made available to the entity that is a user of the system for part or all of the period from January 1 2024 to December 31, 2024 to process their transactions. The criteria we used to make this statement were that the Description:

a. Presents how the system made available to the user entity to process relevant transactions was designed and implemented, including, if applicable:

- The types of services provided, including, as appropriate, the types of transactions processed.
- The procedures, both automated and manual, by which such services are provided, including, as appropriate, the procedures by which they are initiated, authorized,

recorded, processed, corrected as necessary and transferred to reports and other information prepared for entities using the system.

> The information used in the execution of procedures, including, where applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing and reporting transactions; this includes correcting incorrect information and how the information is transferred to reports and other information prepared for the user entity.
> How the system captures and addresses significant events and conditions.
> The process used to prepare reports or other information provided to the system user entity.
> Services performed by a subservice's organization, if any.
> The specified control objectives and controls designed to achieve those objectives, including, as appropriate, the complementary controls of the user entity assumed in the design of the controls of the service organization.
> Other aspects of our control environment, the risk assessment process, information, and communications (including related business processes), control activities and monitoring activities that are relevant to the services provided.

b. The description includes relevant details of changes to the VERIDAS system during the period covered by the description when the description covers a period.

c. The Description does not omit or distort information relevant to the service organization's system, while acknowledging that the Description is prepared to meet the common needs of the system customers.

2. Controls related to the control objectives set out in the Description were properly designed and operated throughout the period from January 1 2024 to December 31, 2024 to achieve those control objectives. The criteria we used to make this statement were that:

> The risks that threaten the achievement of the control objectives set out in the Description have been identified by VERIDAS.
> The controls identified in the Description would provide, if they function as described, reasonable assurance that those risks would not prevent the control objectives set out in the Description from being achieved.
> Controls were applied systematically as designed, including whether manual controls were applied by persons who have the appropriate competence and authority.

ATTACHMENT A- SYSTEM DESCRIPTION

SCOPE

This report describes the control structure of VERIDAS (the "Company") in relation to its “Digital identity verification service & Identity Platform” for the period from January 1 2024 to December 31, 2024 (the "Specified Period"). This report, which includes the description of the controls in this Section, is intended solely for the information and use of the Company, the entities that use the Platform for the entire Specified Period, and the independent auditors of such user entities. This report should not be used by anyone other than these specified parts.

The digital identity verification service and identity platform are designed to meet security, privacy, and compliance requirements.

VERIDAS has an adequate system to provide confidentiality, integrity and availability of customer data. It also provides transparent accountability to enable customers and their agents to track service management.

VERIDAS was born with the purpose of guaranteeing people’s right to use their real identities in the digital and physical world. VERIDAS has a vision of a passwordless and keyless future, where people are recognized privately, securely and voluntarily for who they are. To this end, it develops digital identity verification solutions using its proprietary technologies for identity document verification, facial biometrics and voice biometrics.

VERIDAS main solutions are:

- **Digital Onboarding:** Identity verification for the registration of new clients or the digitalization of existing users. There are different processes according to the regulations and requirements of each sector and each country.
- **Biometric Authentication:** Authorization of online transactions or operations through facial or voice recognition.
- **Fraud Prevention:** Detection of duplicate identities within the customer database to prevent and detect fraud cases.
- **Digital Access Management:** Access control to facilities with facial recognition.

The Identity Platform service was offered by Veridas Access Control Solution during 2023. On March 1, 2024, the company merged with VERIDAS. That involves that solutions, products and services of Veridas were transferred to VERIDAS.

The service facilitates registration with identity verification, biometric access terminals, integration with databases, and a registration and access information analysis system. The solution is an end-2-end that offers a full cycle from the identity verification or register to different access biometric modes, integrations and the management and monitorization of the information involved in the process. In this context, VERIDAS offers versatile solutions that can be used in a wide range of applications such as visitors and employees, sport facilities, gambling, logistics or events. Crucially, the services reduce queues and eliminate the need for physical exchange of documents and credentials.

For these services, the solution has an identity management platform which performs the management of the registration, biometric access terminals and/or an information analysis system, using a state-of-the-art developed in-house. The solution increases security for the client and convenience for the end users.
The registration process can be done remotely or in person, via mobile phone, tablet or computer, such as on-site registration with on-site photo capture, remote registration from the user's device or capture the ID and a selfie. The system verifies the information and reports if the process has been successful (Identity Verification). Remote registration can include identity verification, with identity document verification and biometric matching. Guaranteeing that the user is who they say they are.
The services include design, implementation, manufacturing and maintenance of the hardware (biometric terminals, kiosk, physical barriers control…) that make possible the end-to-end control of personally identifiable data. The way of access through a biometric terminal is fast, convenient and highly secure. The access involves different steps: users approach the biometric terminal, the terminal authenticates the user in less than 1 second, the terminal opens the door and allows them to pass through.

The identity platform handles the fleet of biometric terminals and carries out the identity management for web access. This identity management is based on facial biometric validation as well as document validation (optional). The facial biometric validation uses a state-of-the-art biometric engine developed in-house, continuously improving and regularly submitted for an independent evaluation by the US National Institute of Standards and Technology (NIST), which is the de facto standard in the industry. The facial authentication can be: 1 to 1 verification or 1:N verification. During enrollment, a mathematical representation of the visitor face is generated. Based on these features, VERIDAS streamlines access management, automating all processes involved.

RELEVANT ASPECTS OF GENERAL CONTROL

VERIDAS has implemented several controls within the organization, such as policies, procedures, methods and organizational structure of the organization.

They are detailed in Section III “DESCRIPTION OF THE CONTROL ENVIRONMENT”:

1.1 Control environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

VERIDAS control environment is focused on establishing, enhancing and supervising the effectiveness of specific controls:

- Integrity and ethical values
- Commitment to competence
- Management’s philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices
- Various external influences that affect a Spanish entity’s operation and practices, such as compliance with Organic Law 3/2018, of 5th December 2018, on the Data Protection and Guarantee of Digital Rights and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2 Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.

VERIDAS has placed into operation various processes to identify and manage risks that could affect your clients.

1.3 Information and Communication

Pertinent information must be identified, captured and communicated in a form and

timeframe that enables people to carry out their responsibilities. Information systems deal not only with internally generated data, but also information about external events, activities and conditions necessary for informed business decision making and external reporting.

Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel receive a clear message from top management that control responsibilities must be taken seriously. They understand their own role in the internal control system, as well as how individual activities relate to the work of others. They have a means of communicating significant information upstream. There also needs to be effective communication with external parties.

1.4 Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliation, reviews of operating performance, security of assets and segregation of duties.

1.5 Monitoring and Internal Auditing

Internal control systems are monitored by a process that assesses the performance over time. It is accomplished through both ongoing monitoring activities as well as periodic, separate evaluations. Monitoring controls operate at the entity level as well as at the process level.

VERIDAS monitors the quality and security of internal control performance regarding ISAE 3000, ISO 27001, ENS, ISO 9001 and Data Protection controls.

As a result of the aforementioned control monitoring, reports with the details of the arisen issues and their solution are periodically done.

ATTACHMENT B- DETAILED DESCRIPTION OF THE CONTROL ENVIRONMENT

The digital identity verification service and Identity Platform that VERIDAS offers its clients consists of generic processes tailored to business needs and the technical means required to carry them out. These processes constitute the Information Management System for this service and comprise a set of Control Objectives safeguarding the service quality and the protection and safety of information.

Detailed Descriptions of Controls:

Control Environment:

- The entity has a documented code of conduct that includes its commitments to integrity and ethical values.
- Personnel are required to read and accept the code of conduct upon being hired.
- Personnel are required to read and accept an acceptable use agreement upon being hired.
- New hires are required to pass a background check as a condition of their employment.
- Contractors are required to read and accept the code conduct, read and accept an acceptable use agreement and pass a background check.
- The members of the board of directors are independent of management.
- Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
- The security committee exercises oversight of security controls by reviewing security policies on an annual basis.
- The CISO exercises oversight and independence of risk management activities by reviewing results of internal assessment and third party testing results on an annual basis.
- The security steering committee meets on a monthly basis to discuss security goals, initiatives and projects, including remediation of vulnerabilities.
- The CISO reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.
- An organizational chart has been defined to appropriately document reporting lines in terms of information security.
- Responsibilities for information security have been assigned to all employees
- Job requirements and responsibilities are documented in job descriptions.
- Security awareness training is provided to all employees on an annual basis.
- Managers are required to complete performance appraisals for direct reports at least annually.

- The entity has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
- An architecture diagram exists to document system boundaries to support the functioning of internal control.
- The entity identifies, inventories and classifies virtualized assets.
- A risk assessment is performed on an annual basis to identify and rank potential threats to the system.
- The entity has incident response policies and procedures in place that includes plans for escalating to internal personnel.
- Internal personnel have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel via the employee handbook, which is posted on the company intranet.
- The entity has incident response policies and procedures in place that includes plans for escalating to external personnel.
- The entity communicates its security commitments to external users via customer contracts.
- Agreements are established with key vendors and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners.
- Privacy policies are posted on the entity's website to communicate the entity's privacy practices.
- The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
- When identifying risks to include in the risk assessment, the entity considers relevant laws and regulations specific to the types of data they possess (i.e. Protected Health Information, Personally Identifiable Information, etc.
- Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.
- Management monitors key vendors and business partners on an annual basis by either obtaining and reviewing the vendors' most currently available SOC Reports or by performing other monitoring procedures.
- A risk assessment is performed on an annual basis to identify and rank potential threats to the system.
- Web application scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.
- Web application penetration tests, that include testing for the OWASP top-ten vulnerabilities, are performed by an independent third party on an annual basis and management takes action, as necessary, based on the results of scans.
- AWS-GSUITE-GITLAB and welcome access reviews are performed on an annual basis.
- User activities, exceptions, failures and information security events should be

recorded, protected and periodically reviewed.

- As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.
- Management developed a list of control activities to manage the technology and security risks identified during the annual risk assessment process.
- IT and security policies are defined for protecting against unauthorized access that could compromise the availability, integrity, confidentiality, and privacy of information or systems. IT and security policies are reviewed by appropriate members of management on an annual basis.
- Business and system recovery plans are documented, which provide roles and responsibilities and detailed procedures for recovery of systems to a known state per defined recovery time objectives (RTOs) and recovery point objectives (RPOs). Plans are tested annually.
- Hardening standards are in place to ensure that newly deployed AWS EC2 Instances are appropriately secured.
- Network segmentation is in place so that unrelated portions of the entity's information system are isolated from each other.
- Multi-factor authentication (MFA) is required to access the AWS Management Console.
- Administrator access to AWS is restricted to appropriate personnel.
- AWS password standards are established to enforce the following: password history, minimum length, complexity requirements.
- Internal and external users are required to enter their username and password prior to authenticating to AWS.
- Super user access to AWS is restricted to appropriate internal personnel.
- Employees' access to AWS requires multi-factor authentication.
- Accessing the AWS root account requires MFA.
- Role-based security is in place for internal and external AWS users.
- Customer data at rest is encrypted.
- Full-disk encryption is implemented for all workstations and laptops.
- AWS IAM roles are configured to restrict permissions to cloud resources to appropriate personnel.
- Prior to granting new hires access to system resources, HR must submit a completed access request form.
- New external users are required to agree to the terms of service prior to their account being created.
- A termination checklist is completed by the employee when the contract is terminated to ensure that system access, including physical access, for terminated employees has been removed within one business day..
- When employees transfer to another role, access modifications require a documented

access request form and approval prior to the access being modified.

- A card-based physical access control system has been implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities, including areas containing backup media.
- Administrator access to the physical access control system is restricted to appropriate personnel.
- Visitors must be signed in by an authorized workforce member before a visitor badge that identifies them as an authorized visitor can be issued.
- Hard disk drive destruction policies and procedures have been established for the disposal of hard drives.
- When employees are terminated, workstations are wiped and re-purposed, prior to re-issuing the workstation to another employee.
- Inbound and outbound traffic to AWS is appropriately restricted.
- Anomaly detection for HTTP error codes.
- An intrusion prevention system (IPS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected and perform automated procedures to prevent an intrusion from compromising the network.
- Read/Write access to AWS S3 Buckets are configured to restrict public access.
- AWS automatically logs users out after a predefined inactivity interval and requires users to re-authenticate with their username and password.
- AWS sessions expire when the browser is closed and require the user to authenticate with his or her username and password.
- Web Veridas uses HTTPS to encrypt communications over the internet.
- Customer data is segregated from the data of other customers
- Data loss prevention (DLP) software is used to prevent unencrypted sensitive information from being transmitted over email.
- Removable media devices are required to be encrypted prior to saving files on them.
- Antivirus software is installed on workstations to protect the network against malware.
- Workstations operating system (OS) security patches are applied automatically.
- Virtual machine operating systems are patched on a monthly basis.
- File integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.
- AWS GuardDuty is in place within the cloud environment to detect unauthorized file additions within the cloud environment, server instances, and application containers.
- For code changes, code reviews are performed by someone other than the person who made the code change.
- Cloud infrastructure is monitored through AWS CloudTrail that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.
- AWS CloudWatch is configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.

- The incident response team follows defined incident response procedures for resolving and escalating reported security issues.
- The entity responds to incidents to determine if the incident is considered a security incident and resolution is tracked.
- For all confirmed security incidents, a root cause analysis is performed to determine what corrective actions are necessary to prevent the issue from occurring in the future.
- Incident response plan testing is performed on an annual basis.
- A change management policy is defined to ensure that appropriate controls are in place over the acquisition, development, and maintenance of technology and its infrastructure.
- Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.
- Access to the cloud source code version control system is restricted to appropriate personnel.
- AWS releases are approved by appropriate personnel prior to the release being implemented in production.
- Separate environments are used for testing and production for AWS.
- Developers are restricted from making code changes in production
- Daily backups are performed within AWS.
- Production data is replicated to a different availability zone to provide for recovery of data in the event that the primary availability zone is unavailable.
- The entity has cybersecurity insurance in place to offset the financial impact in the event of a cybersecurity incident.
- Multiple availability zones are utilized in AWS.

Control availability:

- Processing capacity and usage are monitored on a quarterly basis in order to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.
- A load balancer is used to automatically distribute incoming application traffic across multiple instances and availability zones.
- The status of backups is monitored on a daily basis and action is taken when the backup process fails.
- An automated email is sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.
- The integrity and completeness of back-up information is tested on an annual basis.

Control confidentiality:

- The entity establishes written policies related to retention periods for the confidential

information it maintains.

- Customer's data is logically segregated from other customer's data.
- New hires are required to sign a non-disclosure agreement (NDA) upon being hired.
- As part of the employee handbook, a clean desk policy is in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas.
- Test data is used within the AWS test environments.
- Formal policies and procedures are in place to guide personnel in the disposal of paper documents containing sensitive data.
- Paper documents containing sensitive data are placed in a secured storage bin
- Customer data is deleted within the defined days of the customer contract with the entity.

Control processing integrity:

- Application edits limit input to acceptable value ranges
- System edits require mandatory fields to be complete before record entry is accepted.
- The entity identifies information specifications required to support the use of products and services.
- The entity evaluates processing inputs for compliance with defined input requirements in the web application.
- The entity maintains a record of system input activities on the elastic platform.
- Application regression testing validates key processing for the application during the change management process.
- The entity has developed a process to detect behaviour in production different from that expected and to correct them in as it is defined in the inner process.
- The entity records system processing activities of the solution in a single-pane-of-glass observability, including metrics and other security parameters.
- The entity ensures that inputs are processed completely, accurately and timely by processing logs and metrics and by correlating then with appropriate alerts.
- The entity has developed a procedure for log register and metrics to define the system outputs and their processes.
- The entity ensures that system output is only distributed to intended parties by registering them in an environment with different roles and functions/ data ascribed to each customer.
- The entity ensures that system output is complete and accurate by registering the process ascribed to an id identification with allow to inspect them (access, portrayal, onboardings).
- The entity records system output activities related to the user and to the main processed of the system.

Control privacy:

- The entity provides notice of its privacy practices to users prior to users entering information into the web.
- On an annual basis, management reviews the privacy notice to ensure that the privacy notice is accurate.
- The entity communicates privacy practices to customers via the entity's public-facing website.
- The entity's privacy practices posted on the entity's public-facing website includes the following: Purpose for collecting personal information; Choice and consent; Types of personal information collected; Methods of collection (for example, use of cookies or other tracking techniques); Use, retention, and disposal; Access; Disclosure to third parties; Security for privacy; Quality, including data subjects' responsibilities for quality; Monitoring and enforcement.
- Users are required to explicitly agree to the notice of privacy practices prior to entering information.
- The collection of personal information is limited to that necessary to meet the entity's objectives.
- Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.
- The entity maintains policies and procedures that define allowable use and disclosure scenarios.
- On an annual basis, management reviews privacy policies and procedures to ensure that personal information is used in conformity with the purposes identified in the entity's privacy notice.
- Personal information is only used for the purposes identified in the entity's privacy policy.
- Requests for deletion of personal information are captured and information related to the requests is appropriately deleted.
- Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.
- Users accessing their personal information through [application name] must be authenticated with a username and password.
- Users can access all of their personal information.
- Users can correct, amend, or append their personal information by logging.
- Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.
- Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements.
- A documented list of third parties and vendors that are authorized to receive or

access PII is maintained by the Chief Privacy Officer.

- Breaches involving unauthorized uses and disclosures of personal information are tracked and logged in an incident tracking system.
- Incident management procedures include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to the Privacy or Legal department. The entity has a standard incident report template that must be completed for each incident.
- Vendors and third parties with access to personal information are required to sign a formal contract that requires them to notify the entity in the event of actual or suspected unauthorized disclosures of personal information
- Vendors and third parties are provided with information on how to report breaches to the entity.
- The entity has a process for providing notice of breaches and incidents to affected data subjects to meet the entity's objectives related to privacy.
- The entity's privacy practices posted on the entity's website include the list of third parties authorized to receive personal information.
- Users are informed about how to contact the entity with inquiries, complaints, and disputes via the entity's privacy practices that are posted on the entity's public-facing website.
- Data subjects can submit inquiries, complaints, and disputes via the customer portal.
- The entity has a process for tracking users' inquiries, complaints, and disputes within the incident tracking system.
- Executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations.

ATTACHMENT C- PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

VERIDAS makes service commitments to its customers and has established system requirements as part of the Digital identity verification service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. VERIDAS 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 service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements.

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

- **Security**: VERIDAS has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- **Availability:** VERIDAS has made commitments related to percentage uptime and connectivity.
- **Processing Integrity**: VERIDAS has made commitments related to processing customer actions completely, accurately and timely.
- **Confidentiality**: VERIDAS has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

VERIDAS has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and contracts with customers.

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 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 various services.