servis.ai

Overview

Security & Compliance

Quote follow-up email
Not Done
Email
June 1, 2024 5:00 PM
Contact
TAS110409

Todo Follow up call with Matt is due in 15 minutes.
5 minutes ago

Opportunity CAD Medical updated from $4,230 to $6,480.
2 hours ago

Email Boost Your Growth Today to Contact - Matt Jameson opened.
4 hours ago

Report Completed and Emailed: Support Tickets – Monthly.
6 hours ago

Koda Howson added a New Project for Tiger Company.
a day ago

Opportunity Axiom Supply Sales Stage updated from Qualify to Won Selection.
2 days ago

New Ticket TIC1813 assigned to you.
4 days ago

Samantha Kim added a note to Contact Steve Frank.
4 days ago

Hot dog! Another new deal was created. Caring Company – Here we come.
a month ago

Information Security Management ISO 27001 Certified

STAR LEVEL ONE: SELF-ASSESSMENT SECURITY TRUST ASSURANCE & RISK

ADA Tier 2 • CASA Verified

HIPAA COMPLIANT HIPAATraining.com

Table of Contents

Introduction

servis.ai is a fully-featured business operations platform that helps your team get organized, gain visibility into day-to-day work, and get more done with a powerful, easy-to-use sales platform your sales team will actually love. Work smarter and faster with instant visibility, empowering sales teams to do more with less. Speed up cycle times, close more deals, save time, improve business processes, and ensure nothing falls through the cracks by having all your tools in one happy place.

servis.ai Security Focus

servis.ai's primary security focus is to safeguard our customers' data. To achieve this, servis.ai has made substantial investments in implementing the necessary controls to protect and serve our customers effectively. These investments include the establishment of dedicated Product, DevOps, and Security teams. These teams play a crucial role in servis.ai's comprehensive security program and collaborate closely with our Compliance, Legal, and Privacy teams. Together, they ensure the governance process is well-managed. Overseeing the implementation of security safeguards across the servis.ai enterprise is our Chief Technology Officer, who provides strategic oversight and direction to uphold the highest standards of data protection.

Our Security and Compliance Objectives

We have developed our security framework based on industry best practices in the CRM industry. Our key objectives are as follows:

- **Confidentiality and Privacy Assurance:** Our priority is to deliver exceptional products and services while ensuring the privacy and confidentiality of customer data.
- **Service Availability and Business Continuity:** We strive to maintain a high level of service availability and minimize any potential risks that may impact service continuity.
- **Data Integrity and Non-alteration:** We take measures to ensure that customer information remains uncorrupted and is never inappropriately altered.

- **Adherence to Compliance Standards:** We aim to meet or exceed industry standard best practices by adhering to applicable ISO 27001 ISMS controls, HIPAA, and GDPR requirements. Our controls regarding the confidentiality, security, and availability of customer data align with or surpass these standards.

servis.ai Security Controls

In order to protect the data that is entrusted to us, servis.ai utilizes a defense-indepth approach to implement layers of administrative, technical, and physical security controls throughout our organization, leveraging people, processes, and technology. The following sections describe a subset of our most frequently asked-about controls.

Infrastructure Security

Cloud Hosting Provider

servis.ai's corporate offices do not host any production systems or data. Instead, the responsibility of hosting servis.ai's production infrastructure is outsourced to a renowned cloud infrastructure provider, namely Amazon Web Services (AWS). The production infrastructure of servis.ai is securely located within AWS data centers in the United States, which span across multiple availability zones. To ensure the effectiveness of physical, environmental, and infrastructure security controls, we place our trust in AWS's audited security and compliance programs. AWS commits to a service availability guarantee ranging from 99.95% to 100%, which includes redundancy measures for power, network, and HVAC services. To further reinforce our security measures, our internal information security team conducts annual reviews of AWS services, which encompass compliance assessments, audit reports, and assessments of business continuity and disaster recovery plans.

AWS's compliance documentation and audit reports are publicly available at the AWS Cloud Compliance Page and the AWS Artifacts Portal. Customers can obtain AWS compliance and audit reports directly from the AWS Artifact portal. Additional information regarding servis.ai's Cloud Infrastructure can be found on our Cloud Architecture page.

Network and Perimeter Security

The servis.ai product infrastructure enforces multiple layers of filtering and inspection on all connections across our web application firewall (WAF), logical firewalls, and security groups. Network-level access control lists are implemented to prevent unauthorized access to our internal product infrastructure and resources. By default, firewalls are configured to deny network connections that are not explicitly authorized, and traffic monitoring is in place to alert for anomalous activity. Changes to our network and perimeter systems are actively monitored and controlled by our standard internal ticketing system. Firewall rulesets are reviewed by the infosec team on an annual basis to ensure that only necessary connections are configured.

Configuration Management

Automation is the driving force behind servis.ai's ability to scale according to our customers' needs. We have ingrained rigorous configuration management into our day-to-day infrastructure processes. Our product infrastructure operates within a highly automated environment that effortlessly expands its capacity as required.
To ensure reliable operations, we securely store server configurations in images and configuration files. These valuable resources are leveraged to create new server instances with standardized setups. Each instance type has its own meticulously hardened configuration, aligning with the stringent CIS hardening benchmark.

Any modifications or updates made to the configuration and standard images go through a meticulous and controlled change management process. This ensures that all alterations are meticulously tracked, reviewed, and implemented with precision. From the initial provisioning of server instances to their eventual de-provisioning, our system maintains strict control at every stage, fostering a secure and streamlined workflow.
When it comes to patch management, we automate the process or remove server instances that no longer comply with the expected baseline. This proactive approach ensures that our systems remain up-to-date and secure.

Audit logging & Monitoring

The servis.ai application maintains consistent and comprehensive audit logs. These logs are stored in a central logging solution hosted within servis.ai's AWS environment. Security-related logs are specifically retained, indexed, and stored to facilitate investigation and incident response activities.

Write access to the storage service housing the logs is strictly controlled and limited to administrators.

Alerting and Monitoring

servis.ai places significant emphasis on automated monitoring, alerting, and response capabilities to proactively address potential issues. Our product infrastructure is instrumented with CloudWatch, CloudTrail, and Datadog, with instrumentation that triggers alerts to DevOps engineers and the Information Security (InfoSec) team whenever anomalies occur.

CloudWatch, an AWS service, collects and tracks metrics, logs, and events from the application and underlying infrastructure. It triggers alerts to DevOps engineers and infosec teams whenever anomalies occur, such as error rates, abuse scenarios, and application attacks. This allows for prompt investigation, response, and rectification. CloudTrail, another integral component used by servis.ai, logs and monitors API activity within the AWS environment. It provides detailed records of actions taken by users, services, or other AWS resources, enhancing visibility into account activity and aiding in the identification of potential security-related events.

Additionally, servis.ai utilizes Datadog, a powerful monitoring and analytics platform, to further enhance our monitoring capabilities. Datadog enables real-time visibility into system performance, log analysis, and application monitoring. It provides comprehensive alerting capabilities, allowing us to set up custom alerts based on specific thresholds and conditions.

Through the combined utilization of CloudWatch, CloudTrail, and Datadog, servis.ai ensures robust audit logging, monitoring, and automated response capabilities, enabling efficient detection, investigation, and resolution of potential issues.

Application Security

Software Development Lifecycle

servis.ai follows a rigorous Software Development Lifecycle (SDLC) to deliver high- quality software solutions. Our SDLC encompasses various stages, including requirements gathering, design, development, deployment, and maintenance.
Throughout the process, we adhere to industry best practices and employ agile methodologies for flexibility and adaptability. Additionally, our development practice aligns with the guidelines provided by the Open Web Application Security Project

(OWASP), ensuring that security is a top priority. By incorporating OWASP's best practices and recommendations, we proactively address potential vulnerabilities and implement appropriate controls to deliver secure software solutions that protect user data and maintain system integrity.

Code Analysis

At servis.ai, we prioritize code analysis as a vital aspect of our software development process. We employ a comprehensive approach that involves utilizing a mix of open- source and commercial tools throughout our Continuous Integration/Continuous Deployment (CI/CD) pipeline. By leveraging these tools, we ensure a thorough examination of our codebase, promoting the quality and reliability of our software solutions.

Our code analysis practices extend to the mobile application domain as well. We conduct static analysis of both Android and Apple mobile applications to identify potential security vulnerabilities and code quality issues. This meticulous examination helps us proactively address any weaknesses in our mobile applications, ensuring a secure and reliable user experience.

Vulnerability Management

servis.ai is committed to maintaining a robust vulnerability management program to ensure the security and integrity of our systems. As part of this program, we conduct in- house quarterly vulnerability assessments of our web applications and servers, utilizing a combination of open-source and commercial tools. With our in-house capabilities, we proactively identify and address potential vulnerabilities within our infrastructure.

In addition, servis.ai engages third-party experts to perform an annual penetration test on our web applications and systems. These specialized security professionals meticulously identify potential vulnerabilities and weaknesses in our systems and applications. We take prompt action to track and mitigate all identified security issues, prioritizing them based on the severity of the vulnerabilities. Our internal ticketing system ensures that no security concern goes unresolved.

Web Application Defense

Our platform ensures the protection of all customer content through the implementation of a Web Application Firewall (WAF). This WAF tool actively monitors real-time traffic at the application layer and promptly detects and responds to any malicious behavior, either by alerting our team or by denying access based on behavior type and session rate.

To ensure the highest level of security, we have aligned our rules for detecting and blocking malicious traffic with the best practice guidelines provided by the Open Web Application Security Project (OWASP). Specifically, we adhere to the OWASP Top 10 and similar recommendations, which are industry-recognized standards for web application security.

In addition to these measures, we have incorporated protections against Distributed Denial of Service (DDoS) attacks. This means that our products are designed to withstand and mitigate the impact of such attacks, ensuring uninterrupted availability and consistent performance.

Customer Data Protection

Data Classification

servis.ai's tools enable customers to define the type of information to be collected and stored on their behalf. According to the servis.ai Master Subscription Agreement and Acceptable Use Policy, it is the responsibility of our customers to ensure that they capture only appropriate information to support their marketing, sales, services, content management, and operations processes.

Within servis.ai, we have established an internal information classification system that categorizes data into four distinct groups: Sensitive, Confidential, Internal Use Only, or Public. Every piece of information under our control, whether generated internally or received externally, is carefully assigned to one of these categories. Ensuring the highest level of security, all servis.ai employees undergo comprehensive training to fully comprehend the definitions associated with each category and the essential steps required to protect the corresponding information. This policy ensures that any data falling under the Sensitive or Confidential categories is collectively referred to as "sensitive information."

Tenant Separation

servis.ai offers a highly scalable, multi-tenant SaaS solution that ensures logical separation of customer data by utilizing unique tables to associate data and objects with specific customers. The design architecture includes authorization rules, which are consistently validated. Furthermore, we maintain comprehensive logs of application authentication, associated changes, and application availability.

Encryption

All sensitive interactions with servis.ai products, such as API calls and authenticated sessions, are encrypted in transit using TLS version 1.2 or 1.3.

Further, encryption at rest is also implemented. Data stored on servers within our private network is always encrypted using secure AWS KMS technology. The encryption keys are regularly rotated, ensuring that physical access to disk storage is completely secured.

Data Backup and Disaster Recovery

System Resilience and Recovery

servis.ai is dedicated to ensuring 100% availability and zero downtime. With our no scheduled maintenance downtime, our customers can rely on our services to be up and running 24/7 throughout the year. Furthermore, we offer real-time updates and access to historical data on system status through servis.ai's status site.

Further, when it comes to our product services, servis.ai places great emphasis on redundancy. We have painstakingly designed our server infrastructure to be distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure provider. This strategic approach not only guarantees the utmost reliability but also minimizes the likelihood of service disruptions or downtime. Our dedication to redundancy ensures that our customers can experience uninterrupted and seamless service at all times.

Disaster Recovery

servis.ai places great importance on maintaining disaster recovery plans for its key product infrastructure and providers. Additionally, we conduct DR (Disaster Recovery) and fault testing at least once a year, continuously enhancing the DR plan based on the results of these tests. Our dedicated DR team validates the execution of the DR plan by simulating live disaster events through various methods:

- **DR Rehearsals:** The DR team actively engages in practicing mock DR scenarios to ensure the efficiency of the DR plan and identify any significant gaps. After each rehearsal, the team thoroughly reviews the DR plan and collaborates to introduce improvements based on the outcomes of the mock tests.

- **Test Failover:** In a testing environment that closely resembles the production configuration, the DR team performs failover testing to confirm that system recovery can be achieved as outlined in the DR plan. Throughout the failover process, application availability and performance are closely monitored to minimize any impacts and align them with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified in the DR plan.

Backups & Restoration

Automated 7-Day Backup with Point-in-Time Restore:

The servis.ai system integrates automated backups, active for a duration of 7 days. This ensures that customer data and applications are consistently and automatically backed up, offering assurance that their information is continually protected.
Additionally, automated snapshots are performed regularly, and the entire process is managed by AWS Aurora.

servis.ai provides point-in-time restore capabilities, spanning a period that extends beyond the immediate 7 days. This flexibility empowers customers to recover their data or applications to any specific historical state within this extended timeframe. The integrity of customer data is preserved, enabling them to roll back to a known good state whenever necessary.

Efficient Restoration Process:

We understand the urgency of getting our customers' operations back on track after an outage or disaster. Our restoration process is designed for efficiency, with a maximum completion time of just one hour. This includes retrieving necessary backup data and restoring customer systems. Our automated backup system plays a significant role in expediting this process. Additionally, we conduct annual backup restoration tests to ensure the reliability and integrity of our backup data.

Identity and Access Control

Corporate Authentication and Authorization

Access to the servis.ai Corporate network and applications, whether remote on VPN or within the office, requires multi-factor authentication (MFA). Corporate system access is centralized through Single Sign-On (SSO) as a policy. Our password policies adhere to industry best practices, encompassing requirements for length, complexity, rotation, and failed login attempts. We utilize password vaults to manage administrative account passwords, while access to the production infrastructure is governed by Role-Based

Access Control (RBAC) or the JITA process. Furthermore, employee access and permissions to the corporate network and key internal applications undergo regular manual reviews on a monthly and quarterly basis, ensuring that granted access aligns with their job function.

Corporate Security

Background Checks and Onboarding

servis.ai employees in the US and Mexico undergo an extensive third-party background check before receiving formal employment offers. This includes thorough checks on employment history, education, and criminal records for potential employees.

Upon being hired, all employees are required to read and acknowledge servis.ai's Employee Handbook, which includes Information Security requirements. These documents outline employees' security responsibilities in safeguarding company assets and data, ensuring a clear understanding of the expectations in maintaining a secure environment**.**

Policy Management

To ensure a consistent approach to data protection across our organization, servis.ai has established a comprehensive set of written policies and procedures. At the core, we maintain a Written Information Security Policy meticulously designed to align with ISO 27001 requirements. This policy addresses various critical aspects, including data handling requirements, acceptable use of servis.ai assets and information systems, privacy considerations, incident response protocols, and disciplinary measures for policy violations. To uphold the relevance and effectiveness of our policies, they undergo regular review and approval at least once a year. These policies are securely stored within our company's internal portal, providing easy access to all employees and enabling them to stay informed and aligned with our data protection standards.

Security Awareness Training

At servis.ai, we prioritize our employees as the first line of defense in maintaining a secure environment. We are committed to providing comprehensive training to our employees to ensure they are well-prepared for their roles. As part of this commitment, servis.ai employees are required to complete security awareness training within 30 days of joining the company. Furthermore, annual training sessions are conducted to keep employees up-to-date on the latest security practices and initiatives.

In addition to the general security awareness training, we actively keep our employees informed about recent security news and initiatives through internal mailers and our dedicated Slack channel. This ensures that our employees remain knowledgeable and vigilant in identifying and responding to potential security threats.

To further enhance our defense against cyber-attacks, servis.ai conducts phishing awareness training and simulations at least once a year. These exercises help employees recognize and resist phishing attempts, strengthening our overall security posture and supporting our people firewall.

Risk Management

servis.ai has successfully implemented a robust information security risk management process. This includes the documentation of our Information Security Risk Assessment policy and the conduct of an annual risk assessment in collaboration with key departments such as Cloud, Operations, HR, Facilities, and others. The objective of this assessment is to identify and evaluate the information security risks that our organization currently faces. Furthermore, risk mitigation and remediation activities are tracked on the company's internal portal. Additionally, these activities are reviewed by an external auditor as part of the ISO 27001 audit.

Vendor Risk Management

At servis.ai, we prioritize security and privacy through Third-Party Risk Management (TPRM) best practices and vendor due diligence. Our vendor management program includes annual vendor risk assessments, where we inventory, track, and review vendor security programs. We assess safeguards based on services and data exchanged, ensuring ongoing compliance through contractual relationships. Our Security, Privacy, Legal, and Compliance teams collaborate with business stakeholders for comprehensive annual vendor management reviews.

Corporate Physical Security

At servis.ai, we prioritize the security of our offices by implementing multiple layers of protection. In both our US and Mexico locations, we leverage security services to ensure a safe environment for our employees. To control access, we use badge systems tied to individuals, which are promptly de-provisioned in case of loss or when no longer needed, such as during employee terminations, upon notification to our admin team. Additionally, we employ video surveillance and other environmental monitoring measures throughout all servis.ai offices.

Corporate Network Protections

At servis.ai, we prioritize network security by implementing robust controls. All connections between our internal networks and the Internet or any publicly accessible computer network are required to include an approved firewall or related access control system.

The privileges granted through these systems are based on business needs. Our network controls encompass logical segregation of networks into internal, external, and Internet zones, with access and connection restrictions in place. Critical networks, information systems, and applications are protected by firewalls, safeguarding against both external and internal users. These firewalls are configured and managed to grant access only to authorized users.

Endpoint Protection

As part of our comprehensive endpoint protection measures, at servis.ai, company- issued systems and computers are internally managed and configured with full disk encryption. This ensures that data stored on these devices remains secure even in the event of theft or unauthorized access.

Incident Management/ Incident Response

servis.ai information security team has developed a robust procedure that covers a comprehensive range of corporate infrastructure security and privacy events. To aid in incident detection, we utilize various security monitoring tools, including CloudWatch, CloudTrail, and Datadog, which log and generate alerts in case of anomalous activity. Furthermore, we proactively leverage several Open-Source Intelligence (OSINT) tools to discover shadow IT assets, identify externally exposed assets, and assess vendor cyber risk. This allows us to develop proactive incident response activities and mitigate potential threats.

In the event of a security incident, whether suspected or proven, our information security team and leadership conduct a thorough review. We coordinate with affected customers using the most appropriate means based on the nature of the incident. This ensures effective communication, collaboration, and resolution in addressing the incident and minimizing its impact.

Data Breach Response

servis.ai has established a documented data breach response notification process that encompasses data breach reporting policies, procedures, and obligations. This process ensures that in the event of a Personal Data Breach, servis.ai will promptly notify affected customers without undue delay.

We are committed to providing timely and relevant information regarding the breach as it becomes known or as reasonably requested by the customer. Our aim is to maintain transparent and open communication during such incidents to ensure that our customers are kept informed and can take appropriate actions.

Data Privacy

At servis.ai, we prioritize privacy as a fundamental objective in the design and development of our product. Our customer-centric approach ensures that we consider customer needs while upholding the highest privacy standards. Our privacy program is built upon industry best practices and aligns with regulatory requirements, such as GDPR and HIPAA, to ensure compliance.

We are committed to the principle of not selling our customer data to any third parties, as outlined in our privacy policy. This means that your data remains secure and protected, and we prioritize its confidentiality. The protections described in our policies and the measures we have implemented are designed to maintain the privacy and integrity of your data, ensuring it remains private and unaltered.

With our privacy-first approach, you can trust that we take your data privacy seriously and strive to provide a secure and trustworthy experience. In addition, we conduct annual reviews of our privacy policy to ensure its continued relevance and alignment with evolving privacy practices and regulations. This regular review process allows us to make any necessary updates and enhancements to our privacy policy, reinforcing our commitment to protecting your data.

Furthermore, we have appointed a Data Protection Officer (DPO) who oversees our privacy program and ensures compliance with relevant data protection laws and regulations. The DPO plays a crucial role in promoting privacy awareness, providing guidance, and facilitating ongoing adherence to privacy best practices across our organization.

Compliance

ISO 27001

At servis.ai, we are committed to maintaining a strong information security practice that aligns with industry standards. Our information security framework is based on the ISO 27001:2013 standard, which serves as a comprehensive guide for establishing, implementing, maintaining, and continually improving information security management systems. We are proud to announce that servis.ai has achieved ISO 27001 certification, validating our adherence to this globally recognized standard. This certification demonstrates our dedication to protecting the confidentiality, integrity, and availability of information assets, as well as our commitment to maintaining the highest levels of information security across our organization.

As part of this certification, servis.ai undergoes an annual external audit conducted by independent third-party auditors. This audit process rigorously assesses our information security management systems and practices against the ISO 27001:2013 standard, ensuring the ongoing effectiveness and continuous improvement of our information security controls. This annual external audit further reinforces our dedication to maintaining a robust and secure environment for our customer's data.

You can request our ISO 27001 certificate by visiting the following link: FA ISO 27001 report

CSA STAR Level 1

servis.ai proudly holds CSA Start Level 1 certification, demonstrating our commitment to maintaining secure and reliable SaaS services. This certification validates our adherence to industry best practices and ensures the protection of customer data.

For more information or to request our certification, visit https://servis.ai/legal/security/

GDPR

At servis.ai, we place a strong emphasis on compliance with data protection regulations, particularly the General Data Protection Regulation (GDPR).

We have implemented robust measures to ensure that our practices align with the requirements outlined in the GDPR. Furthermore, servis.ai undergoes an annual attestation against GDPR regulations conducted by an independent third-party auditor. This attestation process thoroughly evaluates our adherence to the principles and obligations set forth by the GDPR, such as data subject rights, lawful basis for processing, data protection impact assessments, and data breach notifications. By subjecting ourselves to this annual assessment, we demonstrate our commitment to maintaining the highest standards of data protection and privacy for our customers.

You can request our attestation certificate by visiting the following link: GDPR attestation certificate

HIPAA

servis.ai is compliant with the Health Insurance Portability and Accountability Act (HIPAA). We understand the importance of protecting sensitive healthcare information, and we have implemented comprehensive measures to ensure HIPAA compliance throughout our organization. To further validate our commitment to maintaining the highest standards of data protection in the healthcare industry, servis.ai undergoes an annual attestation conducted by an independent third-party auditor. This attestation process thoroughly assesses our adherence to the privacy, security, and breach notification provisions of HIPAA. By regularly undergoing these assessments, we continuously strive to uphold the privacy and security of protected health information (PHI) and demonstrate our unwavering commitment to HIPAA compliance.

You can request our attestation certificate by visiting the following link: HIPAA attestation certificate

Google OAuth Compliance

servis.ai prioritizes the security of our customers' integration data. As part of our commitment, we annually undergo compliance assessments with integration partners like Google. This ensures that our integration processes are fully compliant with Google OAuth standards, providing a secure environment for our customer's data.

You can request our attestation certificate by visiting the following link: Google OAuth Letter of Assessment