

6SENSE INSIGHTS, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

6SENSE SAAS SUBSCRIPTION SYSTEM

FOR THE PERIOD OF DECEMBER 1, 2024, TO NOVEMBER 30, 2025

Attestation and Compliance Services



Proprietary & Confidential
Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To 6Sense Insights, Inc.:

Scope

We have examined 6Sense Insights, Inc.'s ("6sense") accompanying assertion titled "Assertion of 6Sense Insights, Inc. Service Organization Management" ("assertion") that the controls within 6sense's 6sense SaaS Subscription system ("system") were effective throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that 6sense's 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, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

6sense uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 6sense, to achieve 6sense's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

6sense 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 6sense's service commitments and system requirements were achieved. 6sense has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, 6sense 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 whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems 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.

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 6sense's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve 6sense's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that 6sense'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 6sense's 6sense SaaS Subscription system were effective throughout the period December 1, 2024, through November 30, 2025, to provide reasonable assurance that 6sense's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Tampa, Florida
December 9, 2025

ASSERTION OF 6SENSE SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within 6Sense Insights, Inc.'s ("6sense") 6sense SaaS Subscription system ("system") throughout the period December 1, 2024, to November 30, 2025, to provide reasonable assurance that 6sense's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented below 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 December 1, 2024, to November 30, 2025, to provide reasonable assurance that 6sense's 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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. 6sense's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 December 1, 2024, to November 30, 2025, to provide reasonable assurance that 6sense's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE 6SENSE SAAS SUBSCRIPTION SYSTEM

Company Background

6Sense Insights, Inc., herein referred to as 6sense, is on a mission to revolutionize the way business to business (B2B) organizations create revenue by predicting customers most likely to buy and recommending the best course of action to engage anonymous buying teams. The 6sense agent-powered Revenue intelligence platform, unlocks the ability to create, manage and convert high-quality pipeline to revenue. Customers report 2X increases in average contract value, 4X increases in win rate and 20-40% reduction in time to close deals.

The company was founded in 2013 and has offices in San Francisco, New York, London, Pune, Bengaluru, and Austin. 6sense has financial backing from investors including: Insight Partners, Venrock, Industry Ventures, D1 Capital Partners, Sapphire Ventures, and Tiger Global with Series E funding in 2022.

Description of Services Provided

The 6sense SaaS Subscription leverages artificial intelligence (AI) and big data to provide insights and predictions about customer behavior to arm revenue teams with the data and visibility they need to create and convert high-quality pipeline into revenue. Here are some of the 6sense SaaS Subscription key products and services:

- Platform (ABM): The Platform subscription enables licensed Platform Users to gain insights and execute actions based on these insights such as launching advertising campaigns and activating personalization use cases using 6sense's patented account identification technology to help drive marketing actions.
- Sales Intelligence (SI): This subscription offers sales teams real-time visibility into customer behavior, allowing them to identify the best opportunities and deliver personalized sales outreach. Sales Intelligence (SI) provides services in the form of technographic, psychographic, firmographic, marker intelligence, and contact data ("Business Data") for improving customers sales workflows.
- 6sense Advertising: As an included feature within the 6sense Platform subscription, customers may run advertising campaigns through the Platform to identify and target specific companies, personas, and/or website visitors using our patented 6signal company identity graph technology.
- Orchestration: This subscription enables customers to orchestrate account-based and people-based actions such as automated data enrichment of records, automated new contact acquisition, and automated pushing of targeted audiences to campaigns.
- Data Workflows Enrichment: The 6sense Data Workflows Enrichment subscription enables users to leverage an out of the box canvas with advanced decisioning logic to create real-time, on-demand, or scheduled workflows for enrichment of account, contact or lead objects within data sets in supported CRM systems.
- Predictive: This subscription enables customers to score and prioritize accounts from the customer's CRM and MAP based on 6sense's patented behavioral modeling, profile modeling, and other available data for use by marketing and sales teams.
- Data Packs: A 6sense Data Packs Subscription provides customers a wide selection of purpose-built data flat files ("Files") to fuel customers' go-to-market use cases.
- APIs: 6sense offers a number of Enrichment APIs that deliver enriched data as set forth on the 6sense API Docs Portal here: https://api.6sense.com/docs. 6sense APIs, including Company Identification API and Lead Scoring API, are HTTP-based and allow programmatic communication between 6sense and other applications.
- AI Email: 6sense AI Email allows customers to automate e-mail conversations with prospects and customers using 6sense AI to help create customer-directed automated workflows with responsive replies and workstreams. Note, unique controls for this platform are covered in the 6sense AI Email SOC 2 Type 2 report available on the 6sense trust center.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Principal Service Commitments

6sense has in place operational procedures to help ensure that customer security, availability, processing integrity, confidentiality, and privacy commitments can be met. 6sense commitments to user entities are documented and communicated to customers via the subscription agreement, the 6sense Trust Center, and privacy policy. Confidentiality agreements with customers are documented and enforced prior to sharing any confidential 6sense data. Additionally, 6sense has procedures in place to review documentation from third-party providers to help ensure that they are in compliance with security, availability, processing integrity, confidentiality, and privacy policies.

6sense makes the following security, availability, processing integrity, confidentiality, and privacy commitments to their customers:

- 6sense maintains strong access controls over production systems that store and processes customer data focused on the principle of least privilege.
- 6sense recruits qualified professionals and continuously trains employees to embed security and privacy in all work.
- 6sense continuously monitors people, processes, and technology to ensure the right visibility into risk is maintained and people are accountable for all risks.
- 6sense configures production systems to hardened baseline with changes appropriately reviewed and tested before being implemented.
- 6sense plans for business continuity and information system contingency with regular testing of those plans.
- 6sense ensures people and services are appropriately identified and authenticated before accessing customer data.
- 6sense promptly and appropriately responds to security events and manages incidents to resolution with root cause analysis to reduce the likelihood of repeated events.
- 6sense maintains systems and services to ensure availability of our services to customers.
- 6sense assesses, mitigates, treats, and tracks information security risk at all levels across the organization on a regular basis.
- 6sense evaluates the security and privacy of our critical vendors and sub-processors to ensure the entire supply chain of our services are secure.
- 6sense ensures that data is encrypted at rest within the production boundary and encrypted in-transit when leaving or entering the production boundary.
- 6sense maintains appropriate administrative and technical safeguards to protect the security and integrity of the service and the confidentiality of the customer data.
- 6sense ensures not to disclose, make public or authorize any disclosure or publication of confidential information, except as expressly agreed to in the confidentiality agreement or otherwise in writing by the disclosing party.
- 6sense deletes customer data upon customer request.
- 6sense performs field mapping and data normalization with customer data in order for the service to function.

- 6sense uses collected personal information only for the lawful business purposes for which 6sense collected it including: to provide products, services, or information requested; administrative purposes; research and development; marketing products and services; and other uses allowed by applicable law, such as fulfillment of a legal obligation.
- 6sense shares collected personal information for the following situations or with explicit consent including: with third-party service providers, business partners, subscribers, or affiliates; interest-based advertising and third-party marketing; and as required by law or similar legal purposes.
- 6sense fulfills requests from data subjects to exercise rights, as applicable by jurisdiction, related to the following: being informed on the collection and use of personal information; access to personal information; update or correct personal information; delete personal information; and object to the processing, sale, or sharing of personal information.
- 6sense uses reasonable and appropriate administrative and technical safeguards to secure personal information in accordance with the privacy policy.
- 6sense retains personal information for as long as needed to provide services to 6sense's subscribers, as necessary to fulfill the purposes for which it was collected, or to comply with legal obligations.
- 6sense notifies data subjects electronically of a breach of personal data where required by applicable law.

System Requirements

6sense establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements, including the use of encryption technologies to protect system user data both at rest and in transit, and necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

Such requirements are communicated in 6sense's 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 documents include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the 6sense SaaS Subscription system.

In accordance with 6sense's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users, in each individual case.

Infrastructure and Software

The 6sense SaaS Subscription system is located at facilities hosted by Amazon Web Services (AWS). 6sense does not own or maintain hardware located in AWS data centers and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e., physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer, and storage) and 6sense is responsible for securing the application platform deployed in AWS (i.e., customer data, applications, identity access management, operating system and network virtual firewall configuration, network traffic, and server-side encryption).

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

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
6sense	6sense application	AWS	AWS US East
AWS Identity and Access Management (IAM)	Enables the ability to securely control access to AWS services and resources for users.		
Amazon Elastic Compute Cloud (EC2)	Virtual machines hosting the 6sense application.	EC2 compute instances	
Amazon Elastic Kubernetes Service (EKS)	Managed container service to run and scale Kubernetes containers.	AWS	
Databases	Database used to store customer data and metadata information.	MySQL, RDS, and Singlestore	
Amazon Simple Storage Service (S3)	Highly resilient and available file based datastore for backup, redundancy, and customer artifacts.	AWS	
Networking	Production network services (e.g., WAF, Load balancers, etc.)		
Database Platform	Distributed, relational, SQL managed database service used to store customer data and metadata information.	Singlestore	Singlestore
Identity Management	Federated identity management platform utilized for secure identity management and single sign-on (SSO) capabilities.	Okta	Okta
Identity Verification	User and device authentication	Beyond Identity	Beyond Identity
Virtual private network (VPN)	Utilized to access to the production environment.	Pritunl	Pritunl

Secondary Infrastructure and Supporting Software

The following secondary infrastructure and supporting software is utilized in support of the delivery of the 6sense SaaS Subscription:

- Wiz – cloud security platform for detecting threats, vulnerabilities, misconfigurations, and unusual activity.
- Ox - application security platform for detecting threats, vulnerabilities, and unusual activity.
- Exabeam – security operations platform with security information and event management (SIEM) capabilities for log management, behavioral analytics, and automated threat detection.
- AuditBoard – audit, compliance, and risk management software utilized to automate internal control activities.
- Cobalt – Independent third-party penetration testing services.
- AWS WAF (web application firewall) – WAF utilized to filter web requests and protect the web application from common exploits.

- CrowdStrike – endpoint security software utilized for protection against malware threats and vulnerability exploitation.
- GitHub – source code management software utilized to control code versioning and security through the application development process.
- Harness – continuous integration and continuous delivery (CI/CD) platform utilized for automated testing and deployment.
- Ketch – privacy management platform utilized to track and manage requests related to data subjects.
- Slack – communications platform utilized to facilitate business and operational conversations and alert on configured events.

People

The people at 6sense involved in creating, maintaining, and securing the 6sense systems include, but are not limited to, to following:

- 6sense C-Suite – Executive team responsible for setting goals, holding each organizational unit accountable, and aligning the organization behind centralized initiatives.
- 6sense Security – Responsible for safeguarding the organization's infrastructure, data, and services by implementing and maintaining comprehensive security measures, monitoring for threats, and ensuring compliance with industry standards and best practices.
- 6sense IT Operations – Responsible for managing endpoint devices and corporate IT services to ensure reliable and secure business operations.
- 6sense Engineering – Development and infrastructure teams responsible for creating and maintaining the service software and the production infrastructure within AWS.
- 6sense People – Responsible for the full employee lifecycle, including onboarding, role transitions, offboarding, and essential HR operations.
- 6sense Legal – Responsible for legal matters, including customer contracts, data privacy, and vendor contracting.

Procedures

Access, Authentication, and Authorization

Access to production resources is controlled using permissions associated with 6sense staff and strictly controlled system accounts. Production systems are monitored for deviations from baseline configurations in production environments. In addition, 6sense enforces password complexity requirements and mandates the use of multi-factor authentication (MFA) for access to systems where passwordless authentication is not available. This approach, combined with strict provisioning and de-provisioning protocols, ensures that access to systems is both secure and well-managed, minimizing potential risks to the organization.

In order to access the production environment, users are required to establish connection into the VPN, enforced by MFA, and authenticate via Okta. Users are assigned to various Okta groups for managing access to the production servers, EKS environment, and production databases.

In order to access the AWS console, users must authenticate to the Okta console by passing device-bound authentication as well as entering a one-time generated security code or FIDO2 (WebAuthn).

The in-scope systems are configured to authenticate users with passwordless, device-bound authentication or a unique user account and enforce predefined user account, minimum password, and MFA requirements. Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. Pre-defined security groups are utilized to assign role-based access privileges to corporate resources and segregate access to data based on job function. User access reviews are performed on a quarterly basis to

help ensure that access to customer data is restricted to authorized personnel. Access to stored data located on the production databases is restricted to user accounts accessible by authorized personnel.

Access Requests and Access Revocation

6sense operates an access management process to safeguard system resources and ensure that access is granted only to authorized individuals. The process enforces Role-Based Access Control (RBAC), where access rights are tailored to each user's role and responsibilities, aligning with the principles of least privilege and separation of rights. This ensures that users are provided the minimum necessary permissions to perform their duties, and that sensitive system functions are only accessible to authorized personnel. For any additional access requirements beyond the default role permissions, users need to submit a formal access request via ticketing tool. This request undergoes review and approval by management, ensuring that access is granted only to vetted and appropriate personnel. Access controls are continuously monitored to prevent unauthorized access.

In the event of a termination, 6sense's processes automatically notify the relevant teams to revoke access and recover company assets. As part of the offboarding procedures, access to production systems is promptly terminated for departing employees, ensuring that no unauthorized access persists. Termination tickets are completed, and system access is revoked for employees as a component of the employee termination process.

Security Groups

AWS security groups are defined for the in-scope systems to filter unauthorized inbound and outbound network traffic from the Internet.

Endpoint Management

6sense has established a comprehensive framework to help ensure secure access to production resources from 6sense managed endpoint devices. Each device is recorded in the asset database for effective tracking and accountability. While personal devices are generally restricted for critical activities, exceptions can be granted with prior authorization from management and the security department. Authorized personal devices must comply with stringent security requirements, which include utilizing antivirus software, implementing strong password policies, and adhering to additional security protocols. 6sense ensures that endpoint devices are configured to operate with the latest updated versions of their respective operating systems, guaranteeing that security patches are applied promptly. This contains both operating system updates and authorized application updates.

Documented standard build procedures are utilized for the installation and maintenance of production servers. Production systems are monitored for deviations from baseline configurations in the production environment.

An enterprise endpoint protection solution is utilized to protect registered workstations against malicious software in real-time. Regular reviews of asset inventories and configuration settings are conducted to maintain compliance and ensure the integrity of endpoint security measures.

Change Management

6sense follows documented software development lifecycle and change management standard operating procedures for implementing changes to the 6sense SaaS Subscription system and the underlying infrastructure used to support the services provided. The procedures document and formalize the set of requirements for each phase of the workflow including planning and design, development and testing, deployment, and maintenance. Changes, inclusive of new feature developments, bug fixes, and system optimizations, follow a structured workflow to help ensure quality of code, system, stability, and security. The workflow includes steps to help ensure changes made to in-scope systems are authorized, peer reviewed, tested, and approved prior to implementation. Changes are documented and tracked within a change tracking ticketing system to centrally maintain, manage, and monitor application and infrastructure changes.

Version control software is utilized to restrict access and modification of application and infrastructure source code and provide rollback capabilities. The ability to modify source code and administrative access privileges within the version control software are restricted to user accounts accessible by authorized engineering personnel. Prior to merging code to the main branch, the version control software is configured to enforce independent code review and approval from at least one individual other than the one to initiate the request, as well as successful completion of automated status checks performed within the CI/CD tool. Test results including code analysis, dependency reviews, and security scans, as applicable, are documented within the pull request along with deployment steps.

Development and testing procedures are conducted in a separate environment that is logically segmented from the production environment.

Access privileges to promote changes into the production environment using the CI/CD tool are restricted to user accounts accessible by authorized infrastructure engineering personnel. The CI/CD tool is configured to require approval of the pipeline prior to deployment to production and also configured to alert engineering personnel through the internal team collaboration tool when changes are approved and deployed. In addition, the cloud security platform is configured for file integrity monitoring (FIM) to monitor for changes to the production environment. Administrative access privileges to the FIM tool are restricted to user accounts accessible by authorized security engineering personnel.

Data Backup and Disaster Recovery

6sense production infrastructure is designed to use auto scaling functionality to manage infrastructure capacity, help ensure the availability of services, and prevent delays or errors in the in-scope systems. An automated backup is utilized to perform system backups on a daily basis. Production backup data is replicated to multiple regions to help ensure redundancy and availability. Engineering personnel perform a restoration test of the backup database on at least an annual basis to verify that system components can be recovered from system backups.
6sense has implemented a comprehensive business continuity plan (BCP) to maintain the integrity, availability, and resilience of critical business operations during and after disruptions. The plan focuses on sustaining essential services, protecting employee well-being, and safeguarding company assets and reviewed, updated, and approved on an annual basis.

The BCP includes an annual business impact analysis conducted by the security team, which assesses various threats—natural, human-caused, and technological—to refine recovery objectives and response plans. The plan is activated when significant disruptions, such as disasters or security breaches, compromise service-level agreements or involve third-party service failures. Upon activation, designated leaders oversee communication, response, and recovery efforts to restore normal operations efficiently. To ensure preparedness, annual tabletop exercises simulate potential disruption scenarios, allowing BCP leadership to evaluate the plan's effectiveness and make improvements. Additionally, functional testing of the information system contingency plan (ISCP) includes failover and restore-from-backup scenarios to confirm the resilience of 6sense’s SaaS platform.

System Monitoring

Documented standard build procedures are utilized for the installation and maintenance of production servers. Production systems are monitored for deviations from baseline configurations in production environments. Penetration testing is performed by a third-party vendor on an annual basis to identify threats and assess their potential impact to system security. Security vulnerabilities that are identified are triaged by security personnel and monitored through resolution. WAF is utilized to monitor and analyze web application events and protect against possible or actual DDoS attacks and security breaches.

6sense has implemented a logging and monitoring framework designed to safeguard customer data, maintain compliance, and enhance operational efficiency. Logging and monitoring software is configured to collect data from critical system infrastructure components and endpoint systems to monitor system performance and potential security vulnerabilities and alert the information security team upon detection of unusual system activity or service requests. Each log provides a detailed audit trail, enabling security teams to monitor, detect, and respond to potential threats.

Incident Response

Incident management manual and procedures are in place to prepare for, detect, and respond to platform, security and privacy incidents and reviewed on at least an annual basis. The incident response plan includes details the required steps and actions to triage an incident, understand its impact, and control the damage. In addition, the incident response manual defines the roles and responsibilities of the various departments, standardizes incident phases and categories, promotes prevention of incident recurrence, and promotes continuous improvement. Reported or detected security incidents and their associated responses, including lessons learned, are documented and tracked through resolution. To identify deficiencies in the incident response capabilities and test the awareness of the various team members, an incident management tabletop exercise is conducted on an annual basis. Identified deficiencies and opportunities for improvement from lessons learned are used to implement updates to the related policies and procedures. The Information Security Management System (ISMS) council meets on at

least an annual basis to discuss the effect of identified security issues on the ability to meet business objectives and to identify corrective measures.

Processing Integrity

The 6sense SaaS Subscription requires a valid e-mail address as a component of the registration process prior to establishing an active client account and is configured to perform object data and standardized field synchronization on a daily basis. Additionally, an auto scaling functionality is in place to help prevent processing delays or errors in the in-scope systems.

The 6sense SaaS Subscription is configured to logically segregate customer data environments and automatically restrict access to users assigned to the respective customer's account. Further, the 6sense SaaS Subscription is configured to restrict user access by roles to help ensure accurate data processing.

Privacy Practice Notice and Communication

6Sense operates as a data controller as defined in their privacy policy. 6sense's privacy practice is communicated to the data subjects through the privacy policy available on the company's public-facing website. The policy includes the corporate privacy standards with respect to the purpose for collecting personal information; methods for and sources of collected personal information from third-party sources; use of personal information; disclosure of personal information to third parties; choices available to individuals and the consent to be obtained; and security of personal information and the precautions taken to protect personal information. The privacy policy is reviewed and approved by the legal team on at least an annual basis and if there are any changes to industry requirements, laws and regulations, or business operations and processes. If there are any significant changes to the policy, changes are communicated to the user through notification banners within the platform as well as through e-mails to registered users.

Privacy Practice Choice and Consent

The online privacy policy includes the choices available to users and the consent to be obtained regarding the collection, use, retention, and disposal of personal information. During the registration process and the account set up process, users are required to review and agree to the terms of the privacy policy through the 6sense SaaS Subscription system. The registration process cannot be completed without explicit consent of the privacy policy.

Personally Identifiable Information (PII) Collection

6sense collects personal data through the 6sense SaaS Platform, public-facing websites, and interactions or engagements through other channels. The type of data collected is dependent upon the services and products used and include the following:

- Identifiers such as account information and IP addresses
- Commercial information related to purchases in connection with 6sense services
- Limited information related online activity collected via web analytics such as browsing and search history
- Geolocation IP information regarding approximate device location when visiting 6sense websites
- Inferenced information based on information that has been collected such as purchase preferences and potential future purchase behavior
- User-generated content

Data is collected through various means based on the user's relationship with 6sense. For example, data can be collected when personal information is provided directly through contact forms, interactions with 6sense websites, or posted user-generated content; through recorded calls, training sessions, or webinars; through the use of the platform; and from third-party providers, partners, and integrators who gather data from a variety of sources including data cooperatives and publicly-available sources. 6sense maintains an internal data classification standard to define the data categories, protection levels, and handling measures for information utilized within the in-scope systems and as part of business operations.

PII Use, Retention, and Disposal

Collected data is used by 6sense only for the reasons for which it was collected. As applicable, 6sense only processes personal data when there is a legal basis to do so, as documented within the privacy policy. Uses for collected personal data include the following:

- Fulfilling requests for products, services, or information
- Administrative purposes
- Research and development
- Marketing 6sense products and services
- Processing subscriber-provided information
- Providing business profile information to subscribers and partners for business-to-business marketing and sales purposes

Data is retained and disposed based on the type of data in accordance with documented retention and disposal commitments.

Data Subject Access

The online privacy policy includes multiple methods for data subjects to contact 6sense with inquires, complaints, and disputes including dedicated e-mail addresses, a mailing address, a phone number, and an online privacy center. The privacy center is available on the company's public-facing website for data subjects to submit a web form regarding requests for access to personal information, updates or corrections to personal information, deleting personal information, and objecting to the processing, sale, or sharing or personal information. A privacy management system is utilized to centrally manage data subject requests from the multiple sources and monitor the requests through completion.

Documented data subject request handling procedures are in place to guide personnel in the validation and fulfillment of requests from data subjects. Prior to fulfilling data subject requests, the identity of the data subject is verified. For example, the identity of the data subject can be verified through the use of an expiring link sent to the data subject's e-mail address. If the identity cannot be verified or the request is otherwise defined, the data subjects are notified via the method of inquiry for the reason a request is denied. Further, access to the 6sense SaaS Platform requires users to authenticate via a unique user account and password with minimum requirements. The platform is configured to allow individuals to update user account profiles after initial set up once authenticated.

PII Disclosure and Notification

6sense may disclose personal data to a third-party if the disclosure is required to comply with legal requirements or to enforce 6sense's policies, contracts, and commitments. In the event that 6sense is required to disclose any personal data, 6sense will maintain records of the authorized disclosure and notify the applicable parties. For detected or reported unauthorized disclosures of personal information, 6sense has documented incident response procedures specifically for privacy and legal to address privacy-related incidents including breaches. Incidents are tracked through resolution within a ticketing system. In addition, 6sense has a documented playbook for managing incidents to outline procedures such as breach notification guidelines and templates based on various incident scenarios.

PII Quality, Monitoring, and Enforcement

In order to help ensure that the collected data is accurate and complete, 6sense has implemented the use of various security measures and technical safeguards to protect the personal data. Access to stored personal data located on the production databases is restricted to user accounts accessible by authorized personnel. Confidential personal data is stored in an encrypted at rest format, and the access to encryption keys are also restricted. These privacy-related controls are subject to the internal audit procedures that are performed on an annual basis. The ISMS council meets on at least an annual basis to discuss compliance with the privacy objectives and commitments.

Data

Data Security

6sense prioritizes the security and confidentiality of customer data through a structured data classification standard based on sensitivity of data. This approach ensures that each data type is protected with controls customized to its risk level, reinforcing 6sense commitment to data integrity, privacy, and regulatory compliance. 6sense upholds security of customer data by aligning data handling practices with regulatory standards, conducting background checks for personnel with access to sensitive data, and maintaining clear policies for internal and external disclosures. Confidential data is stored in an encrypted format utilizing AES-256, or better. Access to encryptions keys is restricted to user accounts accessible by authorized personnel. Web servers support TLS 1.2, and higher, encryption for web communication sessions.

Data Retention and Deletion

Documented policies and procedures are in place to guide personnel in the retention of customer data. Data retention commitments are documented and communicated in the customer subscription agreements and data processing addendum. An annual review of the data retention and disposal policy is conducted to ensure customer records are being retained in accordance with 6sense's terms of service. Automated scripts are utilized to retain customer confidential data in accordance with data retention commitments. Documented policies and procedures are in place to guide personnel in the disposal of customer data. Data disposal commitments are documented and communicated in the customer subscription agreements and data processing addendum. Automated scripts are utilized to dispose customer confidential data in accordance with data disposal commitments.

Data Classification

6sense data classification standard organizes data into four tiers, each with specific controls to match its sensitivity:

- Tier 0 (Red): The most sensitive information, including customer data, is strictly limited to authorized personnel.
- Tier 1 (Orange): Regulated data, such as intellectual property and customer support tickets, is managed with robust access control and compliance measures.
- Tier 2 (Yellow): General business data is safeguarded within our network.
- Tier 3 (Green): Public data, with minimal restrictions, remains readily accessible.

Each data tier is governed by stringent protocols. For example, Tier 0 and Tier 1 data must be encrypted both at rest and in transit, with access limited to approved 6sense-managed endpoints.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer Data	Data submitted by or on behalf of the customer such as web traffic information from the customer's website, customer relationship management / marketing automation platform data, platform authentication information, etc.	Tier 0 (Red)
Regulated data	Data subject to laws and regulations that should not be made generally available such as intellectual property, customer support tickets, employee personal data, etc.	Tier 1 (Orange)

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
General Business Data	Data that is created and used in the normal course of business operations such as internal company communications, agreements with vendors and partners, internal policies and procedures, and usage metrics and analytics metadata, etc.	Tier 2 (Yellow)
Public Data	Data that is publicly shareable such as information on the website, API documentation, press releases, product information, etc.	Tier 3 (Green)

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at 6sense, and the types of controls expected to be implemented at AWS to meet those criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
CSOC.01	AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where production systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6, PI 1.2, PI 1.4
CSOC.02	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
CSOC.03	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting and data center hosting services where production systems reside.	CC6.7
CSOC.04	AWS is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where production systems reside.	CC7.2
CSOC.05	AWS is responsible for ensuring capacity demand controls are in place to meet 6sense's availability commitments and requirements.	A1.1
CSOC.06	AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

The following table presents the applicable privacy commitments that require activities to be performed by AWS, alone or in combination with controls at 6sense, and the types of activities expected to be performed at AWS to comply with those privacy commitments.

Ref.	Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
CSOC.07	AWS is responsible for implementing controls to secure handling of personal data, including procedures for data collection, retention, and disposal.	P1.1 - P4.1

Complementary User Entity Control Responsibilities

6sense's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the 6sense SaaS Subscription system and its controls, the following responsibilities should be considered by user entities:

Ref.	Control Activities Expected to be Implemented at User Entities	Related Applicable Trust Services Criteria
CUER.01	User entities are responsible for following the 6sense instance hardening guide to ensure the customer's 6sense instance(s) is configured according to the requirements and risk tolerance of the customer's organization. https://support.6sense.com/knowledge-base/hardening-your-6sense-org/	CC6.1, CC6.3, CC7.3
CUER.02	User entities are responsible for configuring instances to remove the ability for 6sense to view the customer's 6sense instance(s) if instance access by 6sense is not required or desired. Note, enabling this feature may impact support capabilities. https://support.6sense.com/knowledge-base/1500002052742-user-management-rbac/	
CUER.03	User entities requiring professional services or technical support from 6sense to help setup and manage or troubleshoot their instance(s) must configure their instance(s) to allow 6sense personnel edit access for the period required as deemed necessary by the customer. Edit access to customer data is disabled by default. https://support.6sense.com/knowledge-base/1500002052742-user-management-rbac/	
CUER.04	User entities are responsible for requesting 6sense to delete the data.	C1.2, P4.3

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, confidentiality, and privacy categories are applicable to the 6sense SaaS Subscription system.