CloudSense™

Information Security and Compliance Program

Version 1.0

Last Updated: January, 2025

Document Code: CLS-ISC-0122

Legal Notice

The information in these materials is confidential and proprietary of CloudSense and is provided for informational purposes only. CloudSense and its affiliates assume no responsibility for any errors that may appear herein. CloudSense reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of CloudSense to notify any person of such revisions or changes. CLOUDSENSE MAKES NO EXPRESS GUARANTEES OR ANY GUARANTEES IMPLYING LEGAL INTENT WITHIN THIS DOCUMENT. The content of this document is not intended to represent any recommendation on the part of CloudSense.

This document may provide access to or information on content, products, or services from third parties. CloudSense is not responsible for third party content referenced herein or for any changes or updates to such third party sites, and you bear all risks associated with the access to, and use of, such websites and third party content. CloudSense and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Overview

This document summarizes the CloudSense Limited (the “Company”) information security program designed to protect information subject to privacy laws (the “Program”). In particular, this document describes the Program elements pursuant to which the Company intends to (i) ensure the security and confidentiality of covered data, (ii) protect against any anticipated threats or hazards to the security of such data, and (iii) protect against unauthorized access or use of such data in ways that could result in substantial harm to the Company’s customers and their respective clients.

Designation of Representatives

The Company has designated a senior executive with responsibility for security (“Security Officer”). Where an applicable law requires a Data Protection Officer, the organization appoints and maintains such person (“DPO”). The Security Officer is responsible for coordinating and overseeing the Program. IT Compliance provides assistance to the Security Officer and Data Protection Officer or business related to security and the maintenance of the Program. Together, the Security Officer, DPO, and IT Compliance (collectively, the “Privacy Team”) are responsible for coordinating and overseeing the Program. The Privacy Team may designate other representatives of the Company to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to: dpo@cloudsense.com.

Scope of Program

The Program applies to:

1. Information security of Company and customer data.
2. Personally Identifiable Information (PII), personal data, non-public personal financial information, and Protected Health Information (PHI) under applicable laws or customer contracts, whether in paper or electronic form, that is accessed or received by the Company in connection with providing services to its customers (hereinafter "Highly Restricted Data").
3. The security of Company infrastructure and systems, including its software, as well as the Standard Operating Procedures (SOPs) in effect to identify, assess, track and minimize risk, and to consequently maintain all functional requirements.

Risk Identification and Assessment

The Company identifies and assesses external and internal risks to the security, confidentiality, and integrity of the Highly Restricted Data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.

The Company ensures there are appropriate technical and organizational measures to provide a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Company has a process for the selection and implementation of security safeguards to reduce the risks of Highly Restricted Data to reasonable and manageable levels.

The Privacy Team will ensure, on a regular basis, that Company is implementing safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Physical Security

The Company ordinarily utilizes data centers located at Amazon Web Services (AWS) facilities and physical access is heavily controlled by AWS according to its own Information Security policy and specifically its Physical Access controls. Such access is limited to AWS employees and authorized personnel only. Further details on AWS approach and compliance regarding information security and specific certifications/attestations including SOC, ISO 27001, ISO 27017 and ISO 27018 can be found at https://aws.amazon.com/compliance/. For any exceptions to the standard practice of storing the Highly Restricted Data in AWS data centers, the Company ensures that the alternative data center has equivalent or similar physical security measures.

Change Management

The Company has established mechanisms for change management and control to mitigate risks associated with changes to information systems covered by the Change Management Policy. Changes follow defined planning, evaluation, review and approval procedures.

System Access Controls

The Company has established mechanisms for controlled access to its computing resources and data owned or controlled by the Company. The Company enforces business process controls and data classification policies and authorization mechanisms that specify the level of access for a user, a process, or a system.

The Company has also established the requirements for ensuring authorized use of its computing resources via proper user identification and password authentication.

Logging

Logs are established and maintained according to Company practices and contractual requirements with customers. Logs are retained according to the data retention policy.

Password Management Policy

This policy establishes the requirements for ensuring authorized use of the Company's computing resources via proper identification and authentication.

System Administrator and Operational Accounts:

- System administrator (user accounts) or operational accounts are used as part of the system administration function.
- Administrator accounts are kept to the least number possible and only accessible to essential system admin staff.
- Operational accounts are allocated with permissions being set to the minimum level needed to perform the specific operational and system maintenance jobs.
- The passwords for these operational accounts are changed periodically.

Encryption

The Company's services are designed to provide data security and integrity. All services are accessed through encrypted connections using industry standard SSL/TLS. Additionally, the architecture of some of the services provide further security of data by segregating the object data, the indices, and the encryption keys on physically or logically separated systems. Highly

Restricted Data is subject to encryption at rest in accordance with the Company's Encryption Management Policy.

Security Integration in the Software Development Life Cycle

A software application, or software product, typically undergoes several development life cycles, corresponding to its creation and subsequent upgrades. Each such development life cycle constitutes a project. Such projects continue until the underlying technology ages to the point where it is no longer economical to invest in upgrades and the application is considered for either continued as-is operation or retirement. The Company's Product Development team utilizes the Agile software development methodology for development, testing, verification, and validation.

The Company understands that to be most effective, information security must be integrated into the Software Development Life Cycle ("SDLC") from system inception. Early integration of security into the SDLC enables the Company to strengthen its information security practices, through:

- Early identification and mitigation of security vulnerabilities and misconfigurations;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

Patch Management

Networked devices belonging to or managed by the Company are patched with vendor provided operating system security patches. Server patches are applied in a timely manner following appropriate testing of the security patches by the infrastructure team. It is the Company's policy that new devices be patched to the current patch level, as defined by the operating system vendor, when installed in the production network.

Server Hardening

It is the Company's policy to:

(1) Remove unnecessary services, applications, and network protocols. Removing unnecessary services and applications is preferable to simply disabling them through configuration settings because attacks that attempt to alter settings and activate a disabled service cannot succeed when the functional components are completely removed. Disabled services could also be enabled inadvertently through human error.

(2) Configure OS user authentication. For servers, the authorized users who can configure the OS are limited to a small number of designated server administrators. Enabling authentication by the host computer involves configuring parts of the OS, firmware, and applications on the server, such as the software that implements a network service. Lastly, the Company's administrators ensure the appropriate user authentication is in place.

(3) Configure resource controls appropriately. All commonly used server Operating Systems provide the capability to specify access privileges individually for files, directories, devices, and other computational resources. By carefully setting access controls and denying personnel unauthorized access, intentional and unintentional security breaches can be reduced.

Virus Protection

The Company ensures that information used in conducting business is managed such that activity stemming from malicious software (viruses, Trojans, worms, spyware) is prevented or mitigated, unauthorized access to resources and information via malicious software is prevented or mitigated, and availability of the Company's computer resources is not severely impacted by an introduced pathogen.

Anti-Intrusion

The company evaluates the intrusion risk to systems and, where necessary, takes additional measures to mitigate such risk.

Penetration Testing

Penetration is testing a process designed to attempt to compromise a network using the tools and methodologies of an attacker. It involves iteratively identifying and exploiting the weakest areas of the network to gain access to the remainder of the network, eventually compromising the overall security of the network. The Company conducts periodic security testing as a vital way to identify vulnerabilities and to ensure that the existing security precautions are effective and that security controls are configured properly.

We use industry standard tools to carry out internal and external network vulnerability scans and perform web application scans based on the Open Web Application Security Project (OWASP) Top 10. Where appropriate, code security scans are incorporated as part of the development release cycle.

Security Incident Response

The Company has developed and implemented a privacy and security incident response plan designed to provide guidance to employees and contractors on how to report suspected security incidents and violations. Upon becoming aware of a security issue involving Highly Restricted Data, employees and contractors must report the issue immediately to IT Compliance. This plan outlines steps to be taken by compliance management to investigate potential security breaches. These steps include performing a risk analysis of each incident to determine whether the event requires notification per applicable laws and customer contracts. Mitigation and remediation actions are also addressed as part of the incident response activities.

Business Continuity

The Company has established standards, processes, and controls for the timely recoverability of business critical data and information processing systems. These requirements help ensure the continuity of resources that support critical business functions. The Company has also established periodical backup and archive methodologies.

International Data Transfers

The Company has established safeguards for the international transfer of personal data in accordance with applicable data protection laws, such as the European Union’s General Data Protection Regulation. The Company enters into Standard Contractual Clauses with customers as part of the Company's Global Privacy Addendum.

The Company conducts transfer risk assessments where necessary and enters into additional safeguards for the protection of personal data as part of a transfer from the United Kingdom or European Union as warranted by the applicable risk assessment.

Data Disposal

The Company reviews, retains, and disposes of records received or created in the transaction of its business in accordance with regulatory requirements and contractual agreements. The Company works towards eliminating accidental or innocent destruction of records and at the same time, facilitates its operations by promoting efficiency and reducing unnecessary costs of storage of records.

Data Subject Access Rights

The Company has processes and procedures to facilitate the right to access, delete and correct personal data under the GDPR and, to the extent applicable, the California Consumer Privacy Act (“CCPA”), when it is acting either as a controller or processor of personal data.

Training and Education

The Program policies and procedures are communicated to employees and contractors via new hire onboarding and as part of the Annual Information Security Update Program. Notification of significant revisions to existing policies and procedures outside of the on-boarding and the Annual Information Security Update Program are communicated via email to relevant employees and contractors.

The Company has adopted and implemented a sanctions policy designed to address privacy compliance violations by employees. Contractor sanctions are handled per specific contractual processes. This policy and contractual processes address data privacy compliance violations. The Company has also adopted a no retaliation policy that ensures employees who file complaints will not face any retribution for filing complaints for alleged privacy compliance violations.

Overseeing Service Providers

The Privacy Team coordinates with those responsible for the third-party service procurement activities to raise awareness of, and to institute methods for selecting service providers that are capable of maintaining appropriate safeguards for Highly Restrictive Data. In addition, the Privacy Team works with legal counsel to develop and incorporate standard contractual protections applicable to third-party service providers, which will require such providers to implement and maintain appropriate data security safeguards. In addition, these service providers are subject to an annual risk assessment.

Background Check Policy

The Company conducts background checks on applicants for employment and consulting projects in order to determine their suitability in the manner and to the extent permitted by applicable law. Such screening is conducted after a conditional offer of employment or contract has been extended and will generally include collection and review of the applicant's criminal history going back seven years, as well as other relevant information permitted by applicable law, and pursuant to the Company Background Check Policy.

Anti-Slavery Policy

The Company has a zero tolerance approach to slavery and human trafficking and is committed to ensuring that there is no modern slavery or human trafficking in our supply chains or in any part of our business.

The Anti-Slavery Policy Statement is the principal articulation of the Company's policy on slavery and human trafficking. It is intended to inform and influence all of the operational procedures within the Company.

Anti-Bribery and Anti-Corruption Policy

Our Company has zero tolerance for bribery and corrupt activities. The Company complies at all times with applicable anti-bribery and anti-corruption laws, including the U.S. Foreign Corrupt Practices Act and other foreign equivalents.

At all times, our employees and contractors are expected to comply with all applicable laws, including anti-bribery and anti-corruption laws.

Non-Discrimination Policy

It is Company policy to maintain a safe work environment free from discrimination based on race, color, religion or belief, ethnic or national origin, nationality, gender, gender identity, transgender status, sexual orientation, age, physical or mental disability, genetic information, covered veteran status, pregnancy or maternity, marital or civil partner status, or any other status protected by applicable national, federal, state, or local law with regard to any term or condition of employment.

Equal Employment Opportunity Policy

It is Company policy to make all employment decisions regarding recruiting, hiring, promotion, assignment, training, performance assessments, compensation, termination, discipline, and other terms and conditions of employment based solely on an individual's merit, qualifications, and abilities. This Policy applies to all aspects of employment.

Changes to the Program

The Privacy Team is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Company's operations or other circumstances that may have a material impact on the Program.

Document Disclosure

The information contained herein is proprietary to the Company and must not be disclosed to third parties unless they are bound by a Non-Disclosure Agreement. The recipient of this document, by its retention and use, agrees to protect the information contained herein.

Document Maintenance

This document will be reviewed and updated as needed. This document contains a revision history log. When changes occur, the document's revision history log will reflect an updated version number as well as the date, the owner making the change, and change description will be recorded in the revision history log of the document.

Document Revision History

Version #	Author	Revision Date	Change Description
1.0	Compliance Unit	Jan 29, 2025	Creation of initial Information Security Program document.

Document Approval History

Version #	Approved by	Approval Date
1.0	SVP Operations	Feb 06, 2025
1.0	Legal Counsel	Feb 04, 2025