

Data Security Standards

Technical and Organizational Measures for the Raisin Cloud Service

Document Version	09-2026
Review Cycle	Annual
Applies To	All customers of the Raisin Cloud Service
Effective Date	December 1, 2026

This document sets out the Data Security Standards (DSS) in respect of the Cloud Service provided by A.K.A. New Media Inc. (dba Raisin Software) (“Raisin” or “Service Provider”) to Customer pursuant to the Services Agreement. Raisin shall implement the following technical and organizational measures (“TOMs”) in its provision of the Cloud Service.

1. Definitions

Capitalized terms shall have the meanings set forth in this Schedule or elsewhere in the Services Agreement.

1.1. The security and privacy measures for the Cloud Service are designed to protect Customer Data input therein and to maintain the availability of such Customer Data pursuant to the Agreement. Raisin shall treat all Customer Data as confidential by not using, maintaining, or disclosing Customer Data except for purposes of providing the Cloud Service pursuant to the Agreement or as otherwise required by applicable Law, and specifically shall not disclose Customer Data except to Raisin Personnel, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in the Agreement.

Raisin’s Privacy Policy is located here: <https://www.raisinsoftware.org/privacy-policy>.

1.2. Raisin shall securely sanitize physical media intended for reuse prior to such reuse and shall destroy physical media not intended for reuse.

1.3. The TOMs set forth in this Schedule shall be subject to audits as set forth in the applicable Software Schedule for the Software ordered by Customer in an Order. Upon request, Raisin shall provide evidence of stated compliance and accreditation, such as certificates, attestations, and other industry standards as specified in the Agreement, provided that the release of such information would not compromise security for Raisin.

1.4. Additional security and privacy information specific to the Cloud Service may be available elsewhere in the Agreement or the Documentation. Raisin shall direct Customer to available standard Documentation and/or audit reports/certifications if asked to complete Customer-preferred questionnaires or forms, and Customer agrees such Documentation shall be used in lieu of any such

request. Raisin may charge an additional fee to complete any Customer-preferred questionnaires or forms or to provide consultation to Customer for such purposes.

1.5. Compliance and Certifications. Raisin maintains the following security certifications and compliance programs:

- Payment Card Industry Data Security Standard (PCI DSS) Level 1: Raisin has maintained PCI DSS Level 1 Service Provider compliance continuously for over five years and other PCI standards for over 10 years. PCI DSS Level 1 certification reflects independent validation of Raisin's cardholder data environment against payment card industry security requirements.
- SOC 2 Type II: Raisin is actively working toward SOC 2 Type II attestation as part of its 2026 compliance roadmap. SOC 2 Type II provides independent third-party assurance that controls for security, availability, and confidentiality operate effectively on a continuous basis. Customers may request a status update at any time by contacting privacy@raisinsoftware.org.
- ISO/IEC 42001:2023 (AI Management Systems): Raisin is working toward certification under the international standard for AI Management Systems as part of its 2026 AI governance roadmap.

Current certification status and third-party attestations are published and maintained at: <https://trust.raisinsoftware.org>.

2. Security Policies

2.1. Raisin shall maintain and follow IT security policies and practices that are integral to Raisin's business and mandatory for all Raisin employees. Raisin's management shall maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

2.2. Raisin shall review its IT security policies at least annually and amend such policies as Raisin deems reasonable to maintain protection of the Cloud Service and Customer Data processed therein.

2.3. Raisin shall maintain and follow its standard mandatory employment verification requirements for all new hires, including criminal background checks, proof of identity validation, and additional checks as deemed necessary by Raisin and permitted under applicable Law.

2.4. Raisin employees shall complete security and privacy education annually and certify each year that they shall comply with Raisin security and privacy policies.

3. Security Incidents

3.1. Raisin shall maintain and follow documented incident response policies for computer Security Incident handling and shall comply with the data breach notification terms of the Agreement.

3.2. Raisin shall investigate unauthorized access and unauthorized use of Customer Data in connection with or through the Cloud Service of which Raisin becomes aware (a "Security Incident") and shall define and execute an appropriate response plan. Customer may notify Raisin of a suspected vulnerability or Security Incident by submitting a support ticket.

3.3. Raisin shall follow its Incident Response Plan and notify Customer upon confirmation of a Security Incident that is known or reasonably suspected by Raisin to affect the Customer Data, as may be

required by applicable Law or the terms of the Agreement. Such notification shall occur within seventy-two (72) hours of confirmation of the Security Incident or sooner where required by law, including the Retail Payment Activities Act. This timeline applies equally to material incidents caused by AI features. Raisin shall provide Customer with reasonably requested information about such Security Incident and the status of any Raisin remediation and restoration activities.

3.4. Raisin shall follow its Incident Response Plan after becoming aware of a Personal Data Breach with respect to the Cloud Service and shall assist Customer as set forth in Section 9.

4. Access, Intervention, Transfer, and Separation Control

4.1. Raisin shall maintain documented security architecture of networks managed by Raisin in its operation of the Cloud Service, including measures designed to prevent unauthorized network connections to systems, applications and network devices.

4.2. Raisin shall maintain measures for the Cloud Service that are designed to logically separate and prevent Customer Data from being exposed to or accessed by unauthorized Persons. Raisin shall maintain appropriate isolation of its production and non-production environments.

4.3. Raisin shall encrypt Customer Data in transit using industry accepted cryptographic algorithms when transferring Customer Data over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for Customer's secure transfer of Customer Data to and from the Cloud Service.

4.4. Raisin shall encrypt Customer Data at rest using industry accepted cryptographic algorithms. Raisin manages the cryptographic keys and shall maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

4.5. If Raisin requires access to Customer Data, it shall restrict such access to the minimum level required. Such access, including administrative access to any underlying applications, platforms, and infrastructure components ("Components") (collectively "Privileged Access"), shall be individual, role-based, and subject to approval and regular validation by authorized Raisin Personnel following the principles of segregation of duties. Raisin shall maintain measures to identify and remove redundant and dormant accounts with Privileged Access and shall promptly revoke such access upon the account owner's separation or the request of authorized Raisin Personnel.

4.6. Raisin shall maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

4.7. Raisin shall monitor use of Privileged Access and maintain security information and event management measures designed to: (a) identify unauthorized access and activity; (b) facilitate a timely and appropriate response; and (c) enable internal and independent Third Party audits of compliance with documented Raisin policy.

4.8. Logs in which Privileged Access and activity are recorded shall be retained in accordance with the Data Retention Schedule set out in Section 4A of Attachment A (application and access logs: 12–24 months; security and audit logs: the longer of 7 years from creation or 3 years from termination). Raisin shall maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

4.9. Raisin shall maintain computing protections for its end-user systems that include endpoint firewalls, encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

5. Service Integrity and Availability Control

5.1. Raisin shall: (a) perform security and privacy risk assessments of the Cloud Service at least annually; (b) perform penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, annually; (c) enlist a qualified independent Third Party to perform penetration testing at least annually; (d) perform automated management and routine verification of underlying Components' compliance with security configuration requirements; and (e) remediate identified vulnerabilities based on associated risk, exploitability, and impact.

5.2. Raisin shall maintain policies and procedures reasonably designed to manage risks associated with changes to the Cloud Service. Prior to implementation, changes to the Cloud Service shall be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, and documented approval by authorized Raisin Personnel.

5.3. Raisin shall maintain a reasonably up to date inventory of all information technology assets used in its operation of the Cloud Service, monitor and manage the health and availability of the Cloud Service and its underlying Components, and implement, test, and maintain business continuity and disaster recovery plans consistent with industry standard practices.

5.4. Raisin shall maintain measures designed to assess, test, and apply security advisory patches to the Cloud Service and its associated systems, networks, applications, and underlying Components. Implementation of security advisory patches shall be subject to Raisin change management policy.

5.5. Data Back-Up. Raisin shall back up the Cloud Service and Customer Data stored therein daily and copy such back-ups to an off-site location. Back-ups shall be encrypted at rest and during transmission to the offsite location.

5.6. Disaster Recovery. Raisin's service level commitments, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for both standard incidents and Force Majeure Events, are set out in Section 5A of this Schedule.

5A. Service Level Agreement

5A.1. Availability Commitment. Raisin shall use commercially reasonable efforts to make the Cloud Service available at least 99.9% of the time in each calendar month ("Availability Commitment"), measured as: $(\text{Total Minutes in Month} - \text{Excluded Minutes} - \text{Downtime Minutes}) \div (\text{Total Minutes in Month} - \text{Excluded Minutes})$. "Excluded Minutes" means downtime caused by: (a) scheduled maintenance notified to Customer at least 48 hours in advance, not exceeding 8 hours per calendar month; (b) emergency maintenance; (c) Force Majeure Events; (d) acts or omissions of Customer or its Authorized Users; or (e) third-party service failures outside Raisin's reasonable control.

5A.2. Incident Severity and Recovery Time Objectives. For non-Force Majeure incidents, Raisin shall use commercially reasonable efforts to restore the Cloud Service within the following Recovery Time Objectives (RTOs), measured from the time Raisin confirms the incident:

Severity	Definition	RTO
Critical (P1)	Full service unavailability; no workaround possible	1–4 hours
Major (P2)	Significant feature degradation; partial workaround available	4–8 hours
Minor (P3)	Limited impact; workaround exists	24–48 hours

5A.3. Force Majeure Recovery. Where a service disruption is caused by a Force Majeure Event (as defined in the Services Agreement), Force Majeure Events are excluded from the Availability Commitment and standard SLA uptime calculations. Raisin shall use commercially reasonable efforts to restore the Cloud Service within the following objective:

Event Type	RTO
Force Majeure Event (as defined in the Services Agreement)	2 business days from the date Raisin determines restoration is possible

5A.4. Service Credits. If Raisin fails to meet the Availability Commitment in a given calendar month (excluding Force Majeure Events and Excluded Minutes), Customer may request a service credit in accordance with the following schedule, provided Customer submits a written claim within fifteen (15) days of month-end. Service credits are Customer's sole and exclusive remedy for failures to meet the Availability Commitment. Credits are applied against future invoices and are not redeemable for cash. Total credits in any calendar month shall not exceed 50% of the monthly Fees payable for the affected Service. Credits do not apply to Free Services, Payment Processing or Beta Services.

Monthly Uptime	Service Credit	Applies When
Below 99.9%	10% of monthly Fees for the affected Service	Uptime falls below 99.9% Availability Commitment
Below 99.0%	25% of monthly Fees for the affected Service	Sustained or repeated degradation
Below 95.0%	50% of monthly Fees for the affected Service	Severe or prolonged outage

5A.5. Chronic Failure Exit Right. If Raisin fails to meet the Availability Commitment in three (3) or more calendar months within any rolling six (6) month period, Customer may terminate the affected Service for cause on thirty (30) days' written notice and receive a pro-rata refund of any prepaid, unused Fees for the terminated Service, in addition to any earned service credits.

5A.6. Recovery Point Objective. In all cases (Force Majeure or otherwise), Raisin shall restore the Cloud Service using the most recent available backup, with a Recovery Point Objective (RPO) of no more than twenty-four (24) hours of Customer Data loss.

6. Processing of Customer Personal Data

6.1. Processing.

6.2. Customer is (a) a Controller and exporter of any Personal Data that Raisin Processes on behalf of Customer ("Customer Personal Data") or (b) acting as a Processor and exporter on behalf of other Controllers. Customer appoints Raisin as a Processor to Process Customer Personal Data.

6.3. Customer shall comply with all applicable requirements of the Data Protection Laws and will ensure that it has a lawful basis and all necessary appropriate consents in place to enable the lawful transfer of Personal Data to Raisin for the duration and purposes of the Agreement.

6.4. A list of categories of Data Subjects, types of Customer Personal Data, and Processing activities is set out in Attachment A. The purpose and subject matter of the Processing is the provision of the Cloud Service as described in the Agreement.

6.5. Raisin shall Process Customer Personal Data according to Customer's instructions set forth in the Agreement, and, if applicable, Customer's and its Authorized Users' use and configuration of the features of the Cloud Service.

6.6. Customer shall serve as a single point of contact for Raisin. Raisin shall serve as a single point of contact for Customer with respect to its obligations as a Processor under the Agreement.

6.7. Raisin shall comply with all Data Protection Laws applicable to Raisin as Processor. As between the Parties, Customer is responsible for the lawfulness of the Processing of Customer Personal Data.

6.8. Data Subject Rights and Requests. Raisin shall inform Customer of requests from Data Subjects exercising their Data Subject rights (including access, rectification, deletion, and blocking of data) addressed directly to Raisin. Customer shall be responsible for handling such requests. Raisin shall reasonably assist Customer in handling such Data Subject requests in accordance with Section 9.2.

6.9. Third Party Requests and Confidentiality. Raisin shall not disclose Customer Personal Data to any Third Party unless authorized by Customer or required by applicable Law. If a government or Supervisory Authority demands access to Customer Personal Data, Raisin shall notify Customer prior to disclosure, unless such notification is prohibited by applicable Law.

6.10. Return or Deletion of Customer Personal Data. Upon termination or expiration of the Agreement, Raisin shall delete or anonymize Customer Personal Data in accordance with the Data Retention Schedule set out in Section 4A of Attachment A. General platform content and constituent data will be deleted within 1 year of termination. Transaction and financial records will be retained for 7 years from the date of transaction consistent with CRA and IRS requirements. Security and audit logs will be retained for the longer of 7 years from creation or 3 years from termination. All retention is subject to applicable Law and any legal hold obligations.

6.11. Subprocessors. Customer authorizes the engagement of other Processors to Process Customer Personal Data ("Subprocessors"), including all Raisin Affiliates. Raisin shall impose data protection obligations no less protective than those set out in this Schedule on any approved Subprocessor. A current list of Subprocessors, including any third-party AI providers, is publicly maintained at <https://trust.raisinsoftware.org>. Raisin shall notify Customer of any material changes to its Subprocessor list that affect the Processing of Customer Personal Data.

6A. Artificial Intelligence — Processing Controls

This section governs the use of artificial intelligence (AI) tools and third-party AI providers in the provision of the Cloud Service. It supplements the general processing obligations in Section 6 and is consistent with the Data, Privacy & AI Standards published at <https://www.raisinsoftware.org/data-privacy-ai-standards>.

6A.1. Disclosure. Raisin shall disclose to Customer, in the applicable Documentation or Software Schedule, any Cloud Service feature that uses AI to generate, suggest, score, or automate content or recommendations. AI features are clearly labelled within the platform at the campaign configuration level, and Raisin maintains account-level records of which AI features are enabled for each Customer account. Customers may verify the AI feature status for any campaign from within their organization's administration panel.

6A.2. AI Provider Data Processing Agreement. Where Raisin employs third-party AI providers to power Cloud Service features, Raisin shall maintain an enterprise-grade Data Processing Agreement (DPA) with each such provider. Such DPA shall contractually prohibit the AI provider from:

- using Customer Data, donor data, or AI-generated outputs to train, fine-tune, or improve any AI model;
- retaining AI-generated outputs beyond thirty (30) days from generation; and
- disclosing Customer Data or outputs to any unauthorized third party.

A summary of current AI provider DPA protections is published at <https://trust.raisinsoftware.org>.

6A.3. Data Minimization for AI Features. AI features within the Cloud Service are designed to operate with the minimum data necessary. Donor personally identifiable information (PII) — including names, email addresses, and other directly identifying information — is not passed to any third-party AI provider except where strictly required and disclosed in the applicable Documentation.

6A.4. Use of Behavioural and Outcome-Linked Data for Platform Intelligence. Raisin collects anonymized behavioural signals — including engagement patterns, session interactions, form behaviour, and constituent giving outcomes — and uses these signals to train and improve its platform intelligence models (including donor scoring, engagement propensity, and campaign optimization features). These signals are linked to constituent and campaign outcomes at an aggregated level to power Raisin's intelligence capabilities. Where signals are associated with individual giving outcomes for scoring purposes, this is disclosed in the relevant feature documentation. Such signals do not include donor names, email addresses, or other directly identifying personal information. Processing of behavioural and outcome-linked data is conducted in accordance with applicable privacy law, including PIPEDA and Quebec Law 25, and is subject to the same access controls as all Customer Data.

6A.5. No Training on Customer PII. Raisin does not use donor names, email addresses, transaction records, or other directly identifying personal information to train any AI model — its own or any third party's. The behavioural and outcome-linked signals described in Section 6A.4 are processed in a manner designed to prevent re-identification of individual Data Subjects.

6A.6. AI Subprocessors. Any third-party AI provider used by Raisin to deliver AI features constitutes a Subprocessor for the purposes of Section 6.11. Raisin shall notify Customer of any material change to its AI provider relationships that affects the Processing of Customer Personal Data.

6A.7. Human Oversight. No AI-generated output within the Cloud Service is published, transmitted, or acted upon on behalf of a fundraiser or the Customer's organization without a human actively choosing to do so. Customer's administrators retain the ability to disable AI features entirely on any campaign.

6A.8. AI Incident Response. In the event an AI feature causes a material error affecting Customer Data, donor data, or communications, Raisin shall notify Customer within seventy-two (72) hours of confirming the incident. Raisin shall investigate root cause and provide Customer with a written summary of corrective actions taken.

7. [This Section is Intentionally Blank]

8. Audit

8.1. Raisin shall allow for, and contribute to, audits conducted by Customer or another auditor mandated by Customer solely in order for Customer to determine that Raisin is processing Personal Data in accordance with the Agreement, in accordance with the following procedures:

8.1.1. Upon Customer's written request, Raisin shall provide Customer or its mandated auditor with the most recent certifications which Raisin has procured to regularly test, assess, and evaluate the effectiveness of Raisin's Technical and Organizational Measures (TOMs).

8.1.2. Raisin shall reasonably cooperate with Customer by providing available additional information concerning the TOMs reasonably required by Customer to help Customer better understand them.

8.1.3. If further information is needed by Customer to comply with its own or other Controllers' audit obligations or a competent Supervisory Authority's request, Customer shall inform Raisin in writing to enable Raisin to provide such information or to grant access to it. Raisin shall be under no obligation to disclose confidential or commercially sensitive information as part of such audits.

8.1.4. Onsite Audit Rights. The right to conduct an onsite inspection of Raisin's facilities is available only to: (a) Customers whose annual contract value meets the enterprise threshold set out in their Order or Services Agreement; (b) Customers who are required to conduct such an inspection by a competent Supervisory Authority or applicable Law (such as a regulatory audit mandate); or (c) any Customer where Raisin has confirmed a Security Incident directly affecting that Customer's data. Where eligible, such inspections shall be conducted on no less than fourteen (14) days prior written notice to Raisin, during normal business hours, and only in a manner that causes minimal disruption to Raisin's business. Customers not meeting these criteria satisfy their audit rights through Sections 8.1.1 and 8.1.2. Section 9.2 governs cost recovery for assistance beyond standard documentation.

8.2. All audits shall be subject to the auditing party's execution of a confidentiality agreement acceptable to Raisin and shall be conducted at Customer's expense.

8.3. Any auditor mandated by the Customer shall not be a direct competitor of Raisin and shall be bound to an obligation of confidentiality.

8.4. Each Party shall bear its own costs in respect of Section 8.1.1 and Section 8.1.2; otherwise, Section 9.2 applies.

9. Assistance

9.1. Raisin shall assist Customer by TOMs for the fulfillment of Customer's obligation to comply with the rights of Data Subjects and in ensuring compliance with Customer's obligations relating to the security of Processing, the notification and communication of a Personal Data Breach, and the Data Protection Impact Assessment, including prior consultation with the responsible Supervisory Authority if required.

9.2. Customer shall make a written request for any assistance referred to in this Schedule. Raisin may charge Customer no more than a reasonable charge to perform such assistance, such charges to be set forth in a Change Order and agreed in writing by the Parties.

Attachment A: Personal Data Processing Attachment

1. Categories of Data Subjects

Data Subjects of any Customer Personal Data that generally can be processed in the Cloud Service may include Customer's and its Affiliates' employees, contractors, business partners, or customers, and any other Persons whose Personal Data is processed by the Cloud Service. If Customer shall not use the Cloud Service with all the Data Subjects set out above, Customer is responsible for providing complete, accurate, and up-to-date information to Raisin on the actual Data Subjects via Additional Instructions.

2. Personal Data

2.1. Types of Personal Data

- Basic Personal Data (such as name, email, phone, username etc.)
- Activities collected from any Strava integrations
- Data collected from custom profile fields and survey responses
- Images uploaded by fundraising participants of the Customer
- Technically Identifiable Personal Data (such as usage-based identifiers, static IP address, etc. — when linked to an individual)

Customer should not include Personal Data in text fields that are not intended for or do not request Personal Data.

2.2. Special Categories of Personal Data

The Cloud Service was not designed to process any Special Categories of Personal Data.

3. Processing Activities

- Receipt of Customer Data from Data Subjects and/or third parties;
- Computer processing of Customer Data, including data transmission, data retrieval, data access, and network access;
- Technical customer support involving Customer Data at Customer request;
- Transformation and transition of Customer Data as necessary to deliver the Cloud Service;
- Storage and associated deletion of Customer Data; and
- Backup of Customer Data.

4. Duration of Processing

The duration of Processing corresponds to the applicable Subscription Term. Raisin retains different categories of Customer Data for different periods following termination as set out in the Data Retention Schedule in Section 4A below. General platform content is removed within 1 year of termination;

transaction and financial records are retained for 7 years from the date of transaction; security and audit logs are retained for the longer of 7 years from creation or 3 years from termination.

4A. Data Retention Schedule

4A.1. Tiered Retention Schedule. Raisin retains different categories of Customer Data for different periods depending on the nature of the data and applicable legal obligations. The following schedule governs standard retention periods. Where applicable law requires a longer retention period, that longer period applies. Where Customer requests deletion of specific data prior to the end of the applicable retention period, Section 6.2 of this Attachment A governs.

Data Category	Retention Period	Notes
General platform content (fundraising pages, media, campaign data, donor records, constituent data)	Subscription Term + 1 year post-termination	The 1-year post-termination window allows Customer to retrieve data before deletion. See Attachment A, Section 6.1.
Transaction and financial records (donation amounts, tax receipt data, payment records)	7 years from the date of the transaction	Consistent with Canada Revenue Agency (CRA) requirements under the Income Tax Act and U.S. Internal Revenue Service (IRS) requirements under the Internal Revenue Code. Retained to support Customer audit and compliance obligations.
Application and access logs (login events, user activity, feature access)	12–24 months from the date of creation	Retained for security monitoring, incident response, and support purposes.
Security and audit logs (privileged access, administrative actions, system events)	Longer of: (a) 7 years from log creation, or (b) 3 years from termination of the Agreement	Consistent with PCI DSS audit trail requirements and SOC 2 controls. Ensures coverage through any post-termination audit window.
AI-generated outputs	30 days from generation	Outputs processed by Raisin's AI provider are deleted after 30 days. See Section 6A.2.
Anonymized behavioural signals	Indefinite (while non-identifiable)	Used for platform intelligence. Not subject to standard deletion timelines as they do not constitute personal data.

4A.2. Transaction Record Retention Basis. Transaction and financial records are retained for 7 years from the date of the transaction to enable Customer to meet its obligations under the Income Tax Act (Canada) and requirements of the Canada Revenue Agency (CRA), and under the Internal Revenue Code (United States) and requirements of the Internal Revenue Service (IRS), as applicable. Raisin retains these records in its capacity as processor on behalf of Customer and will make them available to Customer upon request to support audit, regulatory, or compliance processes. Retention of transaction records containing Customer Personal Data beyond the general 1-year post-termination window is justified by these legal obligations and is conducted in accordance with applicable privacy law, including PIPEDA and Quebec Law 25.

4A.3. Security and Audit Log Retention. Security and audit log retention applies the longer of: (a) 7 years from the date of log creation; or (b) 3 years from the date of termination or expiration of the Agreement. This approach ensures that logs covering the full term of a Customer relationship remain available through any post-termination audit or investigation window, and is consistent with PCI DSS audit trail requirements and SOC 2 Type II controls.

4A.4. Deletion and Legal Holds. Upon expiry of the applicable retention period for each data category, Raisin shall securely delete or anonymize the relevant data using industry-standard methods. Retention timelines may be extended where data is subject to a legal hold, active litigation, regulatory investigation, or other legal obligation requiring preservation.

5. Technical and Organizational Measures

The TOMs set forth in the Data Security Standards apply to all Customer Data processed by Raisin within the Cloud Service, including Customer Personal Data.

6. Deletion and Return of Data

6.1. During the term of the Agreement, Customer may retrieve Customer Data from the Administration panel, specifically the Reports section, at any time.

6.2. Customer may also request removal of Customer Data (including Customer Personal Data) at any time prior to termination or expiration of the Agreement Term. Customer acknowledges that deletion of constituent data may affect associated fundraising totals, campaign records, reporting data, and other information or data within the Cloud Service that references or is derived from the deleted records. Raisin is not responsible for the impact of Customer-initiated data deletion on historical records or platform-generated reports.

7. Raisin Hosting Locations

Raisin's data hosting locations used for the Cloud Service are based at secure facilities in Canada.

8. Third Party Subprocessors

The Cloud Service involves third party Subprocessors in the Processing of Customer Data, including Customer Personal Data. A current, publicly accessible list of Subprocessors, including all third-party AI providers, is maintained at <https://trust.raisinsoftware.org>.

9. Privacy Contact and Customer Notifications

The general privacy contact for the Cloud Service is privacy@raisinsoftware.org.

Attachment B: API Terms

1. Access to the Raisin API is granted separate from your License and under the conditions outlined in the Licenses & Subscription and Terms of Service of current Agreements. A few important notes related to the Agreement and API are below:

- Any additional support, consulting or services related to the API are not included as part of your Raisin License & Subscription Agreement, and such services are billed.
- One (1) set of access controls (Username and Password) is granted to generate time-based tokens. Successful generation of a token authorizes the recipient to access all organization and constituent data that can be retrieved or posted via available calls (see full documentation: <https://api.akaraisin.com/help>).
- Raisin is not responsible for any disclosure, modification or deletion of your data resulting from access by a non-Raisin application. You are solely responsible for such content and the consequences of data transmission or publication.
- If you intend on providing your access controls to a third-party provider (e.g. developer), please do so securely, and be aware that they are a party to you, your account, and your organization's account data. Any conflicts should be disclosed in a timely manner.
- If you are utilizing the raisin API to process transactions through Raisin's system, additional PCI requirement in your scope for your organization as a shared responsibility. Please see Raisin-Client PCI DSS Responsibility Matrix
- Raisin reserves the right to notify you of additional fees or restrict your access to the API through the course of the current Agreement or in future Agreements.