D A T A S E C U R I T Y

SOC 2 AND ISO/IEC 27001 COMPLIANCE REPORT

Relating to the storage, protection and governance of customer and member data

Document classification: For customer and prospective-customer review

Report date: July 2026

CONTENTS

1. Executive Summary

1.1 Purpose. This report describes the data-security architecture, governance practices, and control environment of a hosted, single-tenant software platform used by member-based organizations to manage sensitive membership records. It explains how data is stored, protected, and governed throughout its lifecycle, and maps the platform's controls to the two assurance frameworks most commonly requested in vendor security reviews: the AICPA SOC 2 Trust Services Criteria and ISO/IEC 27001:2022.

1.2 Foundational design decisions. The platform's security model rests on four foundational design decisions. First, every customer operates in a fully isolated, single-tenant environment — a dedicated database, dedicated file storage, and a dedicated web address — so that no customer's data is ever co-mingled with another's in any shared table or storage bucket. Second, all data is encrypted both in transit and at rest, and access to files is mediated exclusively through signed, time-limited links. Third, access to the application is governed by passwordless, rate-limited authentication combined with granular role-based access control and row-level database security, meaning that authorization is enforced at the data layer itself rather than only at the application layer. Fourth, every record carries a per-record audit trail, and every bulk operation is preceded by a manually saved copy in addition to routine automatic backups, giving both the provider and the customer verifiable accountability and recoverability.

1.3 Residency and prohibited uses. Personal data belonging to members is hosted in Canada on infrastructure that is independently certified against SOC 2 and ISO/IEC 27001. Contractual commitments prohibit the sale of personal data, its use for advertising, and its use to train any third-party artificial-intelligence model. The provider operates as a data processor acting only on the customer's documented instructions, under a data processing agreement designed to satisfy PIPEDA, the GDPR, UK data-protection law, and applicable United States privacy statutes including the CCPA/CPRA.

1.4 Certification status. This report describes a control environment *aligned to* the SOC 2 Trust Services Criteria and ISO/IEC 27001:2022. The underlying hosting and delivery infrastructure is operated by subprocessors holding current SOC 2 and ISO/IEC 27001 certifications, and those attestations are available to customers as part of the audit-response process. Readers conducting formal vendor due diligence should request the provider's current security overview, subprocessor list, and the applicable infrastructure certifications to confirm the assurance artifacts relevant to their own compliance obligations.

2. Scope and Purpose

2.1 Scope. The scope of this report covers the production platform and its supporting services: application hosting and delivery, the managed database and file-storage layer, authentication, transactional and bulk email delivery, error and performance monitoring, and an optional in-application AI assistant. It covers the full data lifecycle — collection and migration, storage and processing, transmission, backup, export, return, and deletion — together with the organizational measures that surround those technical controls: confidentiality obligations on personnel, subprocessor management, breach notification, audit support, and insurance.

2.2 Audiences. The report is intended to serve three audiences. Security and IT reviewers can use Sections 3 through 9 to understand the technical architecture and control implementation. Privacy officers and legal counsel can use Sections 10 through 12 to assess the data-protection posture, processing roles, and international-transfer mechanisms. Procurement and compliance teams can use Sections 13 and 14, which

map the described controls to the SOC 2 Trust Services Criteria and to the Annex A control themes of ISO/IEC 27001:2022.

3. Architecture and Data-Storage Model

3.1 Single-tenant isolation. The platform is architected as a single-tenant system. Each customer is provisioned a dedicated workspace comprising its own isolated database, its own file storage, and its own web address. This is a materially stronger isolation model than the shared-schema multi-tenancy common in SaaS products, where a single database serves many customers and isolation depends entirely on application-layer query filtering. In a single-tenant model, the blast radius of any application-level defect is structurally confined: a query, however malformed, executes against a database that contains only one customer's data. Cross-tenant data leakage — one of the most common and most damaging classes of SaaS security failure — is prevented by architecture rather than merely by code correctness. Tenant isolation is reinforced contractually as well as technically: the service terms commit that customer data will not be co-mingled in any shared table or storage bucket with the data of any other customer, and attempting to breach or circumvent the single-tenant isolation is expressly prohibited conduct for all users of the system.

3.2 Data residency. Member personal records are hosted in Canada, in a Canadian region of the managed database and storage infrastructure. This residency commitment covers the primary categories of sensitive data processed by the platform: names, contact details, employment and classification information, seniority records, dues status, grievance histories, attached documents, and customer-configured custom fields. Limited operational data — such as error diagnostics and email-delivery metadata — may be processed by service providers outside Canada, under contractual safeguards binding those providers. The distinction is deliberate and narrow: the substantive personal records of members remain in-region, while only the telemetry necessary to operate and support the service transits other jurisdictions. Where a customer has a specific regional-hosting requirement, that requirement can be recorded contractually, subject to availability.

3.3 Infrastructure assurance. The platform runs on managed infrastructure providers that hold independent third-party certifications. The database, file-storage, and authentication layer operates on SOC 2 and ISO/IEC 27001-certified infrastructure, with member data pinned to a Canadian region. Application hosting and content delivery run on SOC 2-certified infrastructure. This layered assurance means that physical security, environmental controls, hardware lifecycle management, and low-level network security are attested by independent auditors at the infrastructure tier, while the provider's own controls govern the application, data, and organizational tiers described in the remainder of this report.

4. Data Governance and Processing Roles

4.1 Controller and processor roles. The governance model draws a clear line between the parties' roles. For member data, the customer is the data controller (the “business” under CCPA/CPRA terminology) and the provider is the data processor (the “service provider”). The provider processes member data only on the customer's documented instructions, including instructions given through the platform itself, and is contractually obliged to inform the customer if it believes an instruction would infringe applicable data-protection law. For a narrow category of data — administrator account details and the provider's own billing records — the provider acts as controller in its own right.

4.2 Purpose limitation and prohibited uses. Three prohibitions apply categorically to member data. It is never sold. It is never used for advertising, including “sharing” for cross-context behavioural advertising as defined under the CCPA/CPRA. And it is never used to train any third-party artificial-intelligence model. These are contractual commitments rather than mere policy statements, and they survive as binding obligations for the duration of processing.

4.3 Optional AI functionality. The platform includes an optional in-application AI assistant that customers may enable or disable at their discretion. Its design reflects data-minimization principles: the assistant answers exclusively from product documentation and offer materials, does not access member data, and does not make automated decisions about members. Because member data never enters the assistant's context, the AI feature introduces no additional processing of personal data and no automated-decision-making exposure under Article 22 of the GDPR or analogous provisions.

4.4 Data ownership. Ownership of customer data — including all member data and all outputs derived from it — remains with the customer at all times. The provider's licence to that data is strictly limited: it may host, copy, process, transmit, and display the data solely to the extent necessary to provide, secure, maintain, and support the service. This narrow-purpose licence is the contractual expression of the purpose-limitation principle found in both ISO/IEC 27001's privacy-adjacent controls and the SOC 2 Confidentiality and Privacy criteria.

5. Identity, Authentication and Access Control

5.1 Passwordless authentication. Authentication to the platform is passwordless, using one-time codes delivered by email, and is rate-limited to resist automated attack. Eliminating stored passwords removes the single largest category of credential risk: there is no password database to breach, no password reuse across services to exploit, and no phishable static secret. Rate-limiting the authentication endpoint mitigates brute-force and enumeration attacks against the one-time-code flow itself.

5.2 Role-based access control. Within each workspace, authorization is governed by granular role-based access control comprising forty-seven distinct capabilities distributed across four roles, with permissions scoped by region and branch. This granularity allows customers to implement least-privilege access precisely: an officer responsible for one branch can be limited to that branch's records; a user who needs to view grievances need not be able to modify seniority lists. The customer administers its own access lists and is contractually responsible for keeping them current — an appropriate division of responsibility given that only the customer knows which of its personnel require which access.

5.3 Row-level database security. Beneath the application's role checks, the database itself enforces row-level security. This defence-in-depth measure means authorization is evaluated at the data layer on every query: even if an application-layer flaw were to mis-scope a request, the database's own policy engine would refuse to return rows outside the requesting user's entitlement. Combined with single-tenant isolation, this produces two independent structural barriers between any user and data they are not entitled to see.

5.4 Personnel access. On the provider side, persons authorized to process member data are bound by confidentiality obligations and are granted access strictly on a need-to-know basis. Support access is provided to customer administrators through designated channels, and the provider's contractual commitments prevent it from disadvantaging any customer in maintenance and support relative to others.

6. Encryption and Data Protection in Transit and at Rest

6.1 Encryption. All data is encrypted in transit and at rest. Transport encryption protects every session between users and the platform, and every internal exchange with the managed database and storage layers, against interception and tampering. Encryption at rest protects the stored database and file contents against compromise of the underlying storage media.

6.2 Signed, time-limited file access. File access is mediated through signed, time-limited links. Documents held in the platform's file vaults are never exposed at static, guessable URLs; each access requires a cryptographically signed link that expires after a limited period. This prevents the persistence-of-access problem common to naive file-sharing implementations, in which a link, once generated, remains valid indefinitely and can circulate beyond its intended audience. Under the signed-link model, possession of an old link confers nothing: access must be re-authorized, and re-authorization passes through the platform's authentication and role checks.

7. Auditability, Logging and Monitoring

7.1 Per-record audit trails. Accountability is enforced at the level of the individual record. Every member record carries a per-record audit trail recording changes to it over time, so that the history of any given record — who changed what, and when — can be reconstructed and reviewed. This satisfies both the operational need of customers to supervise their own administrators and the assurance need, under SOC 2 CC7 and ISO/IEC 27001 logging controls, for reliable event records supporting investigation.

7.2 Activity and system monitoring. At the workspace level, the platform provides activity monitoring with session and event logs, giving customer administrators visibility into who accessed the system and what actions were taken. On the provider side, error and performance monitoring instruments the application continuously, so that anomalies, failures, and degradations surface to the engineering team as they occur rather than upon customer report. Structural changes to the organization's data — reorganizations of branches, regions, and executive structures — are themselves tracked with change history, extending auditability beyond individual member records to the customer's organizational configuration.

8. Backup, Resilience and Availability

8.1 Backup regime. The platform maintains automatic backups of each customer workspace on a routine cycle. In addition — and unusually among SaaS providers — a manual copy is saved before every bulk operation. Bulk operations (mass imports, mass updates, large-scale deletions) are precisely the operations most capable of causing widespread data damage in a single action; taking a dedicated pre-operation snapshot means that any bulk action can be rolled back to its immediate prior state without resorting to the most recent scheduled backup and losing intervening work. Bulk imports are further protected at the application layer by conflict detection, preview before commit, and rollback capability. Backups are rotated and expire on a normal cycle, which serves the complementary privacy objective: deleted data does not persist indefinitely in backup archives but ages out on a defined schedule following deletion.

8.2 Availability commitment. The platform carries a contractual availability commitment of 99.9%, measured monthly, with defined exclusions limited to scheduled maintenance for which notice was given, emergency maintenance required to protect security or integrity, and events outside the provider's

reasonable control. The commitment is backed by a tiered service-credit regime, escalating with the severity of the shortfall. Scheduled maintenance is planned outside peak hours where practicable, with advance notice of any maintenance likely to cause material interruption.

8.3 Business continuity and provider-failure protection. The continuity model extends beyond ordinary operations to the scenario customers most fear from any vendor: the provider's own failure. If the provider becomes insolvent, ceases to carry on business, or permanently ceases to maintain a customer's workspace, the customer is contractually entitled, on request, to a current and complete export of its data together with reasonable transition assistance. Combined with the always-available self-service export described in Section 10, this eliminates vendor lock-in as a data-security risk: the customer's ability to recover its own data does not depend on the provider's continued goodwill or solvency.

9. Incident Response and Breach Notification

9.1 Breach notification. The provider commits to notify the customer without undue delay after becoming aware of a personal-data breach affecting member data. Notification is followed, as information becomes available, by details describing the nature of the breach, its likely consequences, and the measures taken or proposed to address it. This staged-disclosure model mirrors the structure of GDPR Articles 33–34 and the breach-reporting provisions of PIPEDA, and is designed so that the customer — as controller — receives what it needs to meet its own notification obligations to regulators and affected individuals within statutory timelines.

9.2 Security suspensions and contact channels. Security-relevant suspension powers are narrowly drawn: the provider may suspend access only where reasonably necessary to prevent material harm arising from a security incident or from prohibited conduct, must limit any suspension to what is reasonably necessary, and must restore access promptly once the cause is resolved. Dedicated contact channels exist for privacy and security matters, separate from general support.

10. Data Lifecycle: Migration, Export, Return and Deletion

10.1 Controlled onboarding and migration. Data enters the platform through a controlled migration process performed by the provider. Critically, no migrated data or configuration goes live in production until the customer has reviewed and approved it in writing. This approval gate functions as a processing-integrity control at the point of highest risk — the initial bulk transfer of an organization's entire records — ensuring completeness and accuracy are verified by the data owner before the migrated dataset becomes operative.

10.2 Continuous self-service export. Throughout the subscription, the customer can export its data — member records, grievance histories, audit logs, and files — to CSV, Excel, or PDF at any time through built-in export functions, without provider involvement or additional charge. Continuous export capability is both a portability control (satisfying data-portability expectations under the GDPR and analogous statutes) and a practical resilience control: the customer can maintain its own independent copies on whatever schedule its policies require.

10.3 Structured exit. On expiry or termination, the exit sequence is deliberately ordered: export first, then revocation of access, then deletion on a schedule agreed and confirmed in writing. At the customer's choice, the provider will either return the data in a commonly used electronic format or delete it and

existing copies, except where retention is required by law. Backups containing the customer's data then expire on the normal rotation cycle following deletion. The sequencing guarantees that access is never cut off before the customer has secured its data, and that deletion, once elected, is complete across live systems and, in due course, backup archives.

11. Vendor and Subprocessor Management

11.1 Disclosed, function-limited subprocessors. The provider engages a small, disclosed set of subprocessors, each limited to a defined function: managed database, file storage, and authentication (member data hosted in a Canadian region, on SOC 2 / ISO 27001-certified infrastructure); application hosting and content delivery (SOC 2-certified infrastructure); transactional and bulk email delivery; error and performance monitoring; and the optional AI assistant, which by design does not access member data.

11.2 Flow-down obligations and customer rights. Each subprocessor is bound by a written contract imposing data-protection obligations no less protective than the provider's own data processing agreement, may use member data only to provide its service to the provider, and the provider remains fully responsible for its subprocessors' performance. Changes to the subprocessor list are subject to advance notice to the customer, with a right to object on reasonable data-protection grounds and a good-faith obligation to address any objection. This combination — a short, transparent list; flow-down contractual obligations; retained provider responsibility; and customer notice-and-objection rights — implements the subprocessor-governance requirements of GDPR Article 28 and the vendor-management expectations of both SOC 2 (CC9) and ISO/IEC 27001 (Annex A supplier controls).

12. Privacy-Law Compliance and International Transfers

12.1 Multi-regime design. The data processing framework is designed to satisfy PIPEDA and substantially similar Canadian provincial legislation, the EU GDPR, UK data-protection law (the UK GDPR and Data Protection Act 2018), and applicable United States federal and state privacy laws including the CCPA/CPRA. Its core commitments track the processor obligations common to these regimes: processing only on documented instructions; confidentiality of personnel; appropriate technical and organizational security measures; subprocessor governance; assistance with data-subject rights; assistance with security, breach notification, data-protection impact assessments, and prior consultation; return or deletion at end of processing; and information and audit support.

12.2 Data-subject rights support. The provider assists the customer, by appropriate technical and organizational measures, in responding to individuals exercising rights of access, correction, deletion, restriction, portability, and objection. If a data subject contacts the provider directly, the provider refers the individual to the customer — the controller — and assists the customer in responding. In practice, much of this assistance is built into the product itself: permissioned member profiles, per-record audit trails, and self-service export mean that access, correction, and portability requests can typically be fulfilled by the customer directly within the platform.

12.3 International transfers. Member data is hosted in Canada. For customers or data subjects in the European Economic Area, the United Kingdom, or Switzerland, transfers to Canada rest primarily on the European Commission's adequacy decision covering Canadian commercial organizations subject to PIPEDA, and equivalent recognitions. Where an adequacy basis is unavailable for a particular transfer, the European Commission's Standard Contractual Clauses — and, for the United Kingdom, the UK

International Data Transfer Addendum — are incorporated by reference and completed with the appropriate particulars. Operational telemetry processed outside Canada is covered by the relevant subprocessors' contractual safeguards, while member personal records remain hosted in Canada.

13. Mapping to the SOC 2 Trust Services Criteria

The SOC 2 framework evaluates a service organization's controls against five Trust Services Criteria: Security (the Common Criteria, mandatory in every SOC 2 report), Availability, Processing Integrity, Confidentiality, and Privacy. The table below maps the control environment described in this report to each criterion.

Trust Services Criterion	Relevant controls described in this report
Security — Control environment & communication (CC1–CC3)	Defined controller/processor roles and documented instructions (§4.1); contractual security commitments and acceptable-use prohibitions (§3.1, §9); confidentiality obligations on personnel (§5.4); dedicated security and privacy contact channels (§9.2).
Security — Monitoring & control activities (CC4–CC5)	Continuous error and performance monitoring (§7.2); activity monitoring with session and event logs (§7.2); audit-response process including security overviews, questionnaires, and infrastructure certifications (§15).
Security — Logical & physical access (CC6)	Passwordless, rate-limited authentication (§5.1); granular RBAC — 47 capabilities across 4 roles, region- and branch-scoped (§5.2); row-level database security (§5.3); single-tenant isolation (§3.1); signed, time-limited file links (§6.2); need-to-know personnel access (§5.4); physical security attested at the certified-infrastructure tier (§3.3).
Security — System operations (CC7)	Per-record audit logging (§7.1); incident detection through monitoring (§7.2); breach notification without undue delay with staged detail (§9.1); narrowly drawn, promptly reversed security suspensions (§9.2).
Security — Change management (CC8)	Customer written approval before any migrated data or configuration goes live (§10.1); scheduled maintenance with notice, off-peak where practicable (§8.2); change history on organizational structures (§7.2).
Security — Risk mitigation (CC9)	Disclosed subprocessor list with flow-down contracts, retained responsibility, and notice-and-objection rights (§11); insurance including technology E&O and cyber-liability coverage (§15).
Availability (A1)	99.9% monthly availability commitment with service credits (§8.2); automatic backups plus pre-bulk-operation snapshots (§8.1); business-continuity export rights surviving provider failure (§8.3).
Processing Integrity (PI1)	Migration approval gate (§10.1); bulk-import conflict detection, preview, and rollback (§8.1); per-record audit trails enabling verification of processing accuracy (§7.1).
Confidentiality (C1)	Encryption in transit and at rest (§6.1); single-tenant isolation with no co-mingling (§3.1); narrow-purpose licence to customer data (§4.4); contractual confidentiality obligations (§5.4); structured return or deletion at exit with backup expiry (§10.3).
Privacy (P1–P8)	Processing only on documented instructions (§4.1); prohibitions on sale, advertising use, and AI-training use (§4.2); data-subject rights assistance (§12.2); breach notification (§9.1); retention limited by exit deletion and backup rotation (§10.3); collection and consent responsibilities allocated to the controller (§4.1).

14. Mapping to ISO/IEC 27001:2022 (Annex A Control Themes)

ISO/IEC 27001:2022 organizes its Annex A controls into four themes: organizational, people, physical, and technological. The table below maps the described environment to representative controls in each theme.

ISO/IEC 27001:2022 control area	Relevant controls described in this report
A.5 Organizational — policies, roles, and cloud governance (5.1–5.8, 5.19–5.23)	Defined processing roles and documented instructions (§4.1); supplier/cloud-service governance with disclosed subprocessors, flow-down contracts, and notice-and-objection rights (§11); contractual security commitments forming the policy baseline (§3, §9).
A.5 Organizational — incident management (5.24–5.28)	Breach notification without undue delay with staged information supply (§9.1); monitoring-driven incident detection (§7.2); dedicated security contact channel (§9.2).
A.5 Organizational — continuity and legal compliance (5.29–5.31, 5.33–5.34)	Backup and snapshot regime (§8.1); availability commitment (§8.2); provider-failure export and transition rights (§8.3); record protection via audit trails (§7.1); multi-regime privacy compliance and transfer mechanisms (§12).
A.6 People (6.1–6.8)	Confidentiality obligations binding all persons authorized to process member data (§5.4); need-to-know access allocation (§5.4); customer responsibility for keeping its own access lists current (§5.2).
A.7 Physical (7.1–7.14)	Physical and environmental security implemented and independently attested at the SOC 2 / ISO 27001-certified infrastructure tier hosting the database, storage, and application layers (§3.3).
A.8 Technological — identity and access (8.1–8.5)	Passwordless, rate-limited authentication (§5.1); granular, scoped RBAC (§5.2); row-level security enforcing authorization at the data layer (§5.3).
A.8 Technological — cryptography and data protection (8.10–8.12, 8.24)	Encryption in transit and at rest (§6.1); signed, time-limited file-access links (§6.2); structured deletion with backup expiry (§10.3); prohibition on secondary uses of member data (§4.2).
A.8 Technological — logging, monitoring, and backup (8.13, 8.15–8.16)	Automatic backups and pre-bulk-operation snapshots (§8.1); per-record audit logging, session and event logs (§7); continuous error and performance monitoring (§7.2).
A.8 Technological — segregation and secure architecture (8.22, 8.26–8.27)	Single-tenant isolation of database, storage, and web address per customer (§3.1); defence-in-depth pairing of application RBAC with database row-level security (§5.3); data-minimizing AI design with no member-data access (§4.3).

15. Ongoing Assurance, Audit Support and Insurance

15.1 Audit support. Assurance is treated as a continuing obligation rather than a point-in-time exercise. The provider makes available the information reasonably necessary to demonstrate compliance with its data-protection commitments — including its security overview and current subprocessor list — and responds to reasonable audits, security checklists, questionnaires, and privacy reviews. Infrastructure-tier assurance can be evidenced through the subprocessors' independent certifications (SOC 2 and ISO/IEC 27001), which cover the physical, environmental, and platform-level controls on which the service is built.

15.2 Insurance and liability. The provider additionally maintains insurance with reputable insurers — including commercial general liability and, as appropriate to the services, technology errors-and-omissions and cyber-liability coverage — and will provide evidence of coverage on reasonable written request. Liability protections for data-protection obligations operate within the contractual liability framework, with carve-outs preserving liability for breach of confidentiality obligations and for gross negligence, wilful misconduct, and fraud.

16. Conclusion

The control environment described in this report reflects a security architecture in which the strongest guarantees are structural rather than procedural. Single-tenant isolation confines each customer's data by design; row-level security enforces authorization at the database itself; passwordless authentication removes stored-credential risk; encryption protects data in every state; signed, expiring links govern every file access; and per-record audit trails plus pre-operation snapshots make every change accountable and reversible. Around that technical core sits a governance framework — processor-only processing on documented instructions, categorical prohibitions on secondary use, disclosed and contractually bound subprocessors, staged breach notification, an export-first exit, and provider-failure continuity rights — that aligns with the SOC 2 Trust Services Criteria across all five categories and with the organizational, people, physical, and technological control themes of ISO/IEC 27001:2022.

For organizations entrusting sensitive membership records to a hosted platform, the combination of Canadian data residency, certified infrastructure, architectural tenant isolation, and enforceable contractual commitments provides a defensible, review-ready basis for vendor approval under both frameworks.
