Let's Build Canadian Football, Together.

BROUGHT TO YOU BY **ASCENSION MEDIA GROUP INC.**

Security Summary

This document describes the technical and organizational security measures **Ascension Media Group Inc.** ("AMGI") implements for the ALL24 platform. It is intended primarily for school board IT reviewers, procurement officers, insurance underwriters, and other parties conducting security review of ALL24 as a vendor.

It is written at the architecture and practices level. Specific technical details such as IP ranges, port numbers, security group rules, and credential management procedures are not disclosed in this document; those details are available under appropriate confidentiality arrangements when required for institutional review.

1. Company and platform

Ascension Media Group Inc. is an Ontario-incorporated company operating the ALL24 platform, a closed, team-scoped Canadian football coaching platform. The company's registered address is 114 Gemini Drive, Hamilton, ON L9C 6C4. **Andrew Miller**, founder, serves as Privacy Officer and Incident Commander.

ALL24 is a web and mobile application accessed by coaches, team staff, and players (aged 13 and older) within their respective team environments. The platform supports film review, playbook design, and team communications.

ALL24 does not require integration with school networks, school-issued single sign-on systems, or installation of software on school devices. There is no on-premises component.

2. Infrastructure architecture

ALL24's user account database and application server both run on Canadian infrastructure. Some media storage and transient video processing occurs on US-based providers, fully disclosed below.

Hosting and data residency

Component	Provider and location
User account database (MariaDB)	**OVH** dedicated server, **Beauharnois, Quebec, Canada**
Application server (PHP / Nginx)	**OVH** dedicated server, **Beauharnois, Quebec, Canada** (same facility as the database)
Encrypted off-site database backups	**AWS S3 — Canada Central region (Montreal)** — encrypted ciphertext only (AES-256-CBC, PBKDF2 600k iterations); the encryption key lives only on the Canadian production server
Film and media storage	**Cloudflare R2** — Eastern North America (ENAM) location preference (may include US data centres)
Transient video processing	**AWS MediaConvert** + S3 — United States; transient files deleted within 48 hours
Push notifications	**Google Firebase** — United States
Payment processing	**Stripe** — direct integration; AMGI does not receive or store payment card data
DNS, CDN, edge	**Cloudflare**

User account data is stored at rest in Canada and is subject to Canadian legal jurisdiction. The application server runs in the same Canadian facility as the database. Data flows between application and database over encrypted (TLS) connections; both endpoints are within Canada.

Media storage on Cloudflare R2 uses the ENAM location preference, which can include Canadian and US data centres; Cloudflare R2 does not currently offer a Canadian-only Jurisdictional Restriction option for this product. Programs requiring strict Canadian-residency for film should contact us before adopting the platform.

Transient video processing on AWS occurs only during the encoding pipeline; transient files are deleted within 48 hours and no persistent media is stored on AWS.

Provider security certifications

AMGI relies on the following independent attestations and certifications maintained by infrastructure providers:

- **OVH Beauharnois (BHS):** ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 (SSAE 18)
- **Cloudflare:** SOC 2 Type II, ISO 27001, ISO 27701, PCI DSS
- **Amazon Web Services (US, transient processing only):** SOC 1 / SOC 2 / SOC 3, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1
- **Stripe:** PCI DSS Level 1, SOC 1 Type II, SOC 2 Type II
- **Google Firebase:** SOC 1 / SOC 2 / SOC 3, ISO 27001, ISO 27017, ISO 27018

AMGI does not hold independent SOC 2 or ISO 27001 certifications at this time. Where institutional reviewers require attestation at the platform layer rather than the infrastructure layer, AMGI is willing to engage with specific compliance questions; comprehensive third-party audit of the AMGI platform is anticipated as the company scales.

3. Encryption

ALL24 uses a **two-layer** encryption-at-rest story for the production user database, with encryption in transit on every public connection.

Data in transit

- All public-facing connections to the ALL24 platform require **TLS 1.2 or higher**.
- Connections from the application server to the user account database run over TLS, with both endpoints inside the same Canadian facility.
- Connections to Cloudflare R2, AWS S3, Stripe, and Firebase are encrypted using each provider's TLS implementations.

Data at rest — Layer 1 (database-wide tablespace encryption)

The MariaDB storage engine encrypts every database file on disk using **AES-256**, including:

- All InnoDB tablespaces (every table in the user account database)
- The InnoDB redo log
- The binary log
- Aria-engine system tables
- Temporary tables on disk
- Temporary files

A copy of the raw database directory yields no readable user data without the encryption key. The key lives in a separate, restricted-access location on the production server (mode 0600, mysql-only) and is never stored in source control, log files, process listings, or backups.

Data at rest — Layer 2 (application column encryption, on top of Layer 1)

The most sensitive data classes are independently encrypted at the application layer, with a *second* key (held separately from the database key):

- **Private message content** — direct messages between users, and chat in live meetings (AES-256-GCM)
- **Pre-account registration submissions** — name, email, phone, mailing address, and free-text notes entered before an account is created (AES-256-GCM)

The combination is deliberate. Layer 1 protects against the physical-disk and stolen-backup threats. Layer 2 protects the highest-sensitivity prose against the much narrower threat where an attacker has both database credentials AND the database tablespace key but not the application key.

Data at rest — backups

Database backups follow the pipeline `mysqldump → gzip → AES-256-CBC encrypt (PBKDF2, 600,000 iterations) → upload`. The encryption happens on the production server before the backup ever leaves the host. Plaintext database content never touches disk on the way out — the only on-disk file is already ciphertext.

Backup files are stored off-site in **AWS S3, Canada Central region (Montreal, Canada)** — under Canadian legal jurisdiction. Because the backup is encrypted on the production server, the off-site copy is ciphertext only — anyone with access to the bucket has unreadable bytes without the backup encryption key, which lives only on the Canadian production server. The S3 bucket access credentials are scoped to a single bucket, IP-restricted to the production server, with no permission to list or read any other bucket.

The backup encryption key is separate from both the tablespace key and the application column-encryption key. Loss of any one key does not compromise the others. Two offline copies of each key are maintained by the platform owner (password manager + physical safe).

Local retention: 7 days on the production server. Off-site retention: 30 days in R2.

Media storage

Cloudflare R2 buckets and AWS S3 buckets used for transient video processing are encrypted at rest using each provider's encryption service.

4. Access control

Application-level access

- Public registration is not available; users must self-register using a Team-issued join code or invite link.
- Each registration enters a "pending" state and requires explicit approval by a Team Administrator or coach before access is granted.
- Role-based access controls separate Team Administrators, coaches, players, and staff within each team environment.
- Cross-team access is not available; users see only the team(s) they have been approved into.
- Direct messages between two users are accessible only to the participants by default; reported messages are reviewable by AMGI administrators only when escalated through the conduct process.

Infrastructure-level access

- The user account database is bound to the local loopback interface only and is not directly reachable from the public internet. The host firewall denies inbound traffic to the database port from any source.
- Database master credentials are stored in a restricted-access credential file and are not embedded in source code.
- Application credentials follow the principle of least privilege — separate credentials for application use and administrative use.
- Cloud provider console access (OVH, Cloudflare, AWS, Stripe, Firebase) is restricted to the founder; passwords are managed in a credential manager and accounts are protected by multi-factor authentication where available at the provider level.
- SSH access to the production server is key-only — no password authentication. `fail2ban` actively bans IPs exhibiting brute-force patterns.

Audit and logging

- Application-level events including registrations, attestations, approvals, and account deletions are logged with timestamps.
- Login events are logged including timestamp and IP address; this is disclosed in the Privacy Policy.
- Cloud provider console access events are logged by each provider.
- Daily log review during routine operations; alarmed for anomalies.

5. Data handling practices

Minimal collection

ALL24 collects only the personal data required to operate the platform: full name, email address, optional profile avatar, roster information (team, position, jersey number), and attestation records. The platform does not collect dates of birth, home addresses, phone numbers, academic records, health information, or government-issued identifiers.

Retention

- Active accounts: data retained for the duration of active platform use
- Voluntary departure from a team: team-scoped data (chat, watch history) retained for a 14-day grace period, then permanently stripped
- Coach-initiated removal: access revoked immediately; team-scoped data enters a 48-hour reinstate window for correction of mistakes, then permanently stripped
- Account deletion: 30-day grace period for restoration, then permanent deletion
- Inactive accounts (never joined a team): auto-deleted after 90 days
- Inactive accounts (previously attached to a team): auto-deleted after 12 months from last activity
- Chat messages: rolling 12-month retention
- Suspended team accounts (non-payment): data retained for 12 months for reinstatement, then deleted

Right of access and deletion

- Users can download a complete archive of their account data through their account settings (**Settings → Privacy → Download my data**), including registration details, attestation history, agreements accepted with timestamps, login history, watch history, and chat messages. The archive is a ZIP file with one JSON per data class plus a human-readable summary.
- Users can delete their account at any time through account settings or by contacting privacy@all24.ca.
- Account deletion implements PIPEDA's right of access + deletion with a 30-day grace period for accidental deletion.

De-identification

After data is stripped on team departure or account deletion, certain operational metrics may be retained in de-identified form (e.g., aggregate engagement counts, total messages posted in a time window). De-identified metrics contain no name, email, team association, or other identifier that could reasonably link the data back to an individual.

6. Incident response and breach notification

AMGI maintains documented processes for both operational incidents and privacy breaches:

Privacy Breach Notification Process v1.1. Defines the assessment criteria (RROSH framework), containment procedures, notification timeline (72 hours for breaches involving real risk of significant harm), notification templates for affected individuals and the Office of the Privacy Commissioner of Canada, and the internal breach log structure. Available on request to qualified institutional reviewers.

Incident Response Process v1.1. Defines four-tier severity classification (P1 Critical / P2 High / P3 Medium / P4 Low), detection and response procedures, communication standards, rollback options, and the internal incident log structure. Available on request to qualified institutional reviewers.

Both processes operate under a single-operator response model at AMGI's current scale, with the founder serving as Privacy Officer and Incident Commander. External privacy counsel is engaged as needed for assessment of significant or ambiguous incidents.

7. Backup and recovery

- Daily encrypted database backups (AES-256-CBC + PBKDF2 600k iterations), with 7-day local + 30-day off-site retention
- Backups uploaded to AWS S3 (Canada Central, Montreal) as ciphertext only — backup encryption key never leaves the Canadian production server
- Source code maintained in version-controlled repositories; recoverable to any prior state
- Recovery objectives: for P1 incidents involving the database, target recovery within hours; for application-server-level incidents, recovery within minutes via deployment rollback
- Disaster recovery posture: in the event of a catastrophic loss of the production server, the database is independently backed up off-site and source code is independently maintained, allowing reconstruction on alternative infrastructure

8. Vendor and sub-processor management

AMGI uses a small set of established infrastructure providers, each disclosed in the ALL24 Privacy Policy. Each provider operates under its own data processing terms, privacy commitments, and security certifications. AMGI does not engage providers without published privacy practices, and does not engage providers known to use customer data for unrelated purposes.

AMGI reviews its provider list at minimum every six months as part of the semi-annual security review, and updates the Privacy Policy and this Security Summary if providers are added, changed, or removed. Material changes are communicated to users through the platform.

9. Application security practices

- Standard practices for input validation, output encoding, and protection against common web application vulnerabilities (cross-site scripting, SQL injection, cross-site request forgery)
- Authentication uses password-based login with **Argon2id** (modern memory-hard hashing algorithm; winner of the Password Hashing Competition)
- Session management with reasonable session timeouts and rotation
- Code dependencies updated regularly; security advisories monitored and addressed
- Production deployments are versioned and rollback-able
- Sensitive credentials are managed via secret management practices and not embedded in source code

AMGI has not yet undergone external penetration testing or third-party security audit. These are anticipated activities as the company scales. Specific testing or audit requests from institutional reviewers can be discussed on a case-by-case basis.

10. User safety and conduct

Given that the platform may be used by minor athletes, ALL24 implements specific safety controls:

- Age gate at registration (13 or older required); attestation of parental permission required for users 13–17
- No public profiles, no cross-team visibility, no contact with users outside the team
- Team chat is visible to all team members and coaches
- Direct messages between users are private to participants but reportable; reported messages are reviewable by AMGI through the conduct escalation process
- Direct messages do not allow image sharing — text only
- Reporting functionality is available throughout the platform
- Coach approval gating ensures Team Administrators control who can join the team
- 5-report escalation threshold automatically escalates a user to AMGI administrators for review

11. Security review cadence

AMGI conducts a **semi-annual security review** approximately every six months. The first review is scheduled for the **end of November 2026** (post-football-season). The review covers infrastructure changes, vendor list, the breach log, the incident log, application security practices, and policy documents (Privacy Policy, Terms of Service, Team Agreement, Privacy Breach Notification Process, Incident Response Process, this Security Summary).

Findings are documented internally. Material changes to security practices or vendor relationships are reflected in the Privacy Policy and this Security Summary, and are communicated to users through the platform.

12. Contact for security inquiries

- General security inquiries: privacy@all24.ca
- Privacy Officer: Andrew Miller, Founder, Ascension Media Group Inc.
- Address: 114 Gemini Drive, Hamilton, ON L9C 6C4
- Vulnerability reports: responsible disclosure of suspected vulnerabilities to security@all24.ca with subject prefix "SECURITY:". AMGI commits to acknowledging receipt within 72 hours and coordinating remediation in good faith with the reporter.

13. Revision history

- **v1.1 — May 2026** — Updated to reflect post-2026-05-02 architecture (OVH Quebec for both database and application server), the two-layer encryption at rest (database-wide tablespace + application-level Tier 1 columns), and the self-serve user data export feature.
- **v1.0 — May 2026** — Initial version. Establishes baseline architecture, encryption, access control, data handling, and security review cadence.

Privacy: privacy@all24.ca · General: support@all24.ca

all24.ca · Ascension Media Group Inc. · Hamilton, Ontario

This Security Summary describes Ascension Media Group Inc.'s security practices for the ALL24 platform. It is provided for institutional review and may be shared with school boards, insurance underwriters, and other interested parties under appropriate use.

Document version: May 2026 · v1.1