MindBank

DATA PROTECTION & SECURITY

How we keep your *information safe.*

Technical and organizational protections

A project and social enterprise of

ElevateHER Mental Health Support Services Canada

Internal operational policy · Version 1.0 · April 2026

HOW TO READ THIS DOCUMENT

Promises *made operational.*

The Privacy Policy tells the people whose data we hold what we do with it. This document tells everyone inside MindBank — staff, contractors, developers, advisors — how to actually do those things, technically and operationally.

This is the document that makes our privacy commitments real. If you have access to MindBank systems or data, you are bound by everything in here.

It is for the project lead, the developer, the clinical reviewer, editorial staff, advisors with platform access, subscribing organizations (Section 8 specifically), funders and auditors reviewing our security posture, and future board members or Ethics Council.

01. The principles behind every security decision

1.1 Data minimization is the first defense

The most secure data is data we never collected. Every system, form, and process is designed to capture only what's needed for current operational purposes. When in doubt, we don't collect.

1.2 Defense in depth

No single security control is perfect. We layer protections so that compromising one layer doesn't compromise the data — encryption, access controls, monitoring, staff practices, vendor controls, and incident response all work together.

1.3 Least privilege

Every person and every system has the minimum access required for its function. Access is reviewed regularly and revoked promptly when no longer needed.

1.4 Auditability

Every consequential action on personal data is logged, with the actor, the timestamp, and the action. We can answer the question "who accessed this person's information, and when?" for any contributor, at any time.

1.5 Honest incident response

Breaches will happen to any organization that exists long enough. When they do, we respond honestly, quickly, and learn publicly. We do not minimize, delay notification, or attempt to contain the optics rather than the breach.

02. Data classification

Not all data needs the same level of protection. We classify data into four levels, and apply controls appropriate to each.

Level 4 — Highly sensitive (most restrictive)

- Pre-screening conversation notes
- Clinical reviewer assessments
- Contributor banking and tax information
- Records of consent withdrawals and the circumstances around them
- Records related to contributor wellbeing concerns
- Privacy breach investigation records

> *Access: Project lead and clinical reviewer only. Each access logged.*

Level 3 — Sensitive

- Contributor identifying information (name, email, address)
- Subscribing organization contact information and contracts
- Original (un-anonymized) contribution drafts
- Editorial communications between contributors and staff
- Contributor agreements and signed consent records
- Demographic information about applicants and contributors

> *Access: Project lead, clinical reviewer, and editorial staff with role-based scope.*

Level 2 — Internal

- Anonymized contribution content (post-publication)
- Subscriber access logs (which content viewed, by which org)
- Aggregate platform analytics
- Internal operational records (workplans, financial planning, partnership notes)

> *Access: All MindBank staff and contractors as needed for their role.*

Level 1 — Public

- Published anonymized content (visible to authenticated subscribers)
- Public website content
- Published transparency reports
- Public versions of our policies (privacy, ethics, terms)

2.1 Default classification

When data classification is unclear, default to the highest applicable level until reviewed. It is always safer to over-protect than under-protect.

03. Technical protections

3.1 Where data lives

- **Primary database:** Supabase, Canadian region (ca-central-1)
- **Backups:** Encrypted, retained 90 days, same Canadian region
- **File storage:** Supabase Storage, Canadian region
- **Email:** Google Workspace (Canada-based service, Canadian data residency election where available)
- **Analytics:** Privacy-respecting analytics (Plausible or self-hosted equivalent), Canadian or EU-only data

No personal data is stored on US-based servers, third-party advertising platforms, or services that do not commit to Canadian data residency.

3.2 Encryption

- **In transit:** TLS 1.3 for all connections to MindBank systems. No fallback to older protocols.
- **At rest:** AES-256 encryption for all stored data. Database disk encryption, file storage encryption, backup encryption all enforced at the platform level.
- **Sensitive fields:** Additional application-level encryption for the most sensitive Level 4 fields (banking information, social insurance numbers if collected for tax purposes).

3.3 Access controls

- **Authentication:** Multi-factor authentication required for all accounts with access above Level 1.
- **Database access:** Row Level Security (RLS) policies enforced at the database level, so that even a compromised application layer cannot bypass access rules.
- **Role-based permissions:** Each role (project lead, clinical reviewer, editor, developer) has defined permissions documented in our access matrix (Appendix A).
- **Service accounts:** Each integration (payment processor, email, etc.) has a unique service account with minimum required permissions.
- **No shared accounts:** Every login is attributable to a specific person.

3.4 Monitoring and logging

- **Database access logs:** All Level 3 and Level 4 data access is logged with timestamp, user, action, and record affected.
- **Authentication logs:** All login attempts (successful and failed) are logged.
- **Anomaly review:** Logs are reviewed monthly by the project lead. Anomalies are investigated within 5 business days.
- **Retention:** Logs are retained for 12 months, then archived for an additional 12 months.

3.5 Backups and recovery

- **Frequency:** Continuous database backups via point-in-time recovery; full daily snapshots
- **Encryption:** All backups encrypted at rest with the same controls as primary data
- **Testing:** Recovery procedures tested quarterly; restore actually performed at least annually
- **Retention:** 90 days, then permanently destroyed
- **Geographic location:** Same Canadian region as primary data; no cross-border replication

3.6 Software and dependency management

- **Updates:** Critical security patches applied within 7 days of release for production systems
- **Dependencies:** Reviewed quarterly for known vulnerabilities (using tools like Dependabot, npm audit)
- **New dependencies:** Vetted before adoption — license, maintenance status, security history reviewed
- **Removed dependencies:** Decommissioned dependencies removed from the codebase rather than left dormant

3.7 Network and infrastructure

- **Production access:** Restricted to specific IP allowlist where feasible
- **Development environments:** No production data in development or staging environments. Test data is synthetic.
- **API access:** All API endpoints require authentication. Rate limiting in place to prevent abuse.
- **DDoS protection:** Enabled at the hosting layer (Netlify/Cloudflare for public site, Supabase for application)

04. Organizational protections

4.1 Onboarding

Before being granted access to any MindBank data above Level 1, every person:

1. **Signs a confidentiality agreement** specific to MindBank, covering data handling expectations and the consequences of breach
2. **Completes privacy training** covering PIPEDA basics, MindBank's specific obligations, and the contents of this document
3. **Acknowledges the access matrix** in writing — the specific data they are and are not authorized to access
4. **Receives credentials through secure channels** (never via plain email or messaging)

> *No exceptions. Even short-term contractors complete this process.*

4.2 Ongoing practice

- **Quarterly access reviews:** Project lead reviews all access lists; revokes anything no longer needed
- **Password management:** All credentials stored in a password manager (1Password or equivalent), never in plain text
- **Device security:** Personal devices accessing MindBank data must have full disk encryption, screen lock, and current OS security updates
- **Public Wi-Fi:** Access to MindBank systems from public Wi-Fi requires VPN
- **Incident reporting:** Any suspected security issue must be reported to the project lead within 24 hours

4.3 Offboarding

When a person's role with MindBank ends, within 24 hours:

1. **All system access is revoked**
2. **Any MindBank data on personal devices is deleted** (verified by the person under confidentiality obligation)
3. **Confidentiality obligations continue indefinitely** after departure
4. **Final access review documented**

4.4 Vendor and contractor due diligence

Before engaging any vendor or contractor with potential access to personal information, we:

1. **Review their security practices** through documentation or questionnaire
2. **Verify Canadian data residency** for any service that will process identifiable data
3. **Sign a Data Processing Agreement (DPA)** that binds them to MindBank's standards

4. **Limit data access** to the minimum needed for the engagement
5. **Review annually** — vendor security practices can degrade over time

Vendors who refuse to sign a DPA or who cannot demonstrate adequate practices are not engaged, regardless of feature advantages or cost.

05. Roles and responsibilities

5.1 Privacy Officer (Stephanie Atwood, Project Lead)

The Privacy Officer is the single accountable person for MindBank's privacy and data protection posture. Specific responsibilities:

- Final accountability for all decisions in this policy
- Responding to privacy requests from data subjects within statutory timelines
- Receiving and triaging incident reports
- Approving access changes
- Liaising with the Office of the Privacy Commissioner of Canada when required
- Conducting annual security reviews and reporting findings

5.2 Developer (contracted)

- Implementing and maintaining technical controls described in Section 3
- Documenting technical architecture decisions
- Reviewing dependency security quarterly
- Implementing breach detection and notification mechanisms
- Available to support incident response within agreed SLA

5.3 Clinical reviewer (contracted)

- Maintaining confidentiality of all contributor information they access
- Documenting clinical observations within the secure platform, never on personal devices
- Reporting any data access anomalies they observe

5.4 Editorial staff and contractors

- Accessing only the contributions assigned to them
- Following anonymization protocols documented in the Operating Framework
- Reporting any breach or near-miss promptly

5.5 All persons with access

Everyone with access has these baseline responsibilities:

- Following the controls in this policy
- Reporting concerns or incidents promptly
- Not sharing credentials
- Not transferring MindBank data to personal accounts or devices
- Treating all MindBank data as confidential by default

06. Incident response

6.1 What counts as an incident

Any of the following triggers our incident response process:

- Confirmed unauthorized access to MindBank data
- Suspected unauthorized access (anomaly that cannot be quickly explained)
- Loss or theft of a device containing MindBank data
- Email or document containing personal information sent to the wrong recipient
- Disclosure of personal information beyond what consent authorized
- Vendor or service provider notifying us of a breach affecting our data
- Any information system vulnerability that could lead to data exposure

6.2 Immediate response (within 4 hours of discovery)

1. **Contain:** Limit further exposure (revoke access, take systems offline if necessary, change credentials)
2. **Document:** Begin a written incident log with timestamps
3. **Notify the Privacy Officer** if the incident was discovered by anyone else
4. **Preserve evidence:** Don't delete logs, communications, or system state that may be relevant

6.3 Investigation (within 24-72 hours)

1. **Determine scope:** What data was involved, how many people, what types of information
2. **Determine cause:** Technical, organizational, or external
3. **Assess risk:** What's the realistic harm to affected individuals
4. **Document findings** in writing

6.4 Notification

To affected individuals: Within 72 hours of confirmation, where the breach creates a real risk of significant harm. Notification includes what happened, what information was involved, what we are doing in response, what the affected person can do to protect themselves, how to contact us, and their right to complain to the OPC.

To the Office of the Privacy Commissioner of Canada: Where required by PIPEDA — generally, where the breach creates a real risk of significant harm. Reports filed via the OPC's official process.

To subscribing organizations: If a breach affects subscriber data, within 72 hours.

Public notification: For breaches affecting more than a small number of individuals, or where public awareness would help affected people protect themselves.

6.5 Remediation and learning

After every incident:

1. **Root cause analysis** completed within 30 days
2. **Prevention measures** identified and implemented
3. **Policy updates** made if the incident reveals a gap
4. **Public reporting** in the next annual transparency report (without identifying individuals)

> *We do not punish people who report incidents in good faith. Punishment for honest mistakes drives reporting underground, which is the opposite of what we need.*

07. Specific operational practices

7.1 Email and messaging

- **Sensitive information by email:** Avoid where possible. When necessary, use end-to-end encrypted email or a secure shared document instead of email body.
- **No personal information in subject lines.** Ever.
- **Reply-all discipline:** Triple-check recipients before sending anything containing personal information.
- **Mistaken sends:** Treated as incidents under Section 6. Recall attempts and follow-up notification required.

7.2 Physical documents

- **Print only when necessary.** Most operations should be paperless.
- **Secure storage:** Any physical document containing personal information stored in a locked drawer or cabinet.
- **Shredding:** Personal information is cross-shredded when no longer needed.
- **Travel:** Documents containing personal information do not leave the office without explicit authorization.

7.3 Video and audio recordings

- **Pre-screening conversations:** Recorded only with explicit, documented consent. Stored on Canadian-region servers. Deleted after notes are taken (typically within 7 days).
- **Recorded interviews (contribution format):** Recorded with explicit consent. Used only for the agreed editorial purpose. Retained per agreement.
- **No covert recording.** Ever, by anyone.

7.4 Communications about contributors among staff

- Use working names or contributor IDs, not full names, in routine internal communications
- Never discuss contributors in public spaces (cafés, public transit, video calls in shared spaces)
- Use the secure platform for case-specific notes, not personal email or messaging

7.5 Demonstrations and presentations

- Never use real contributor information in demos
- Use synthetic test data for any external demonstration
- Anonymized published content can be used in presentations only if doing so respects the contributor's stated geographic and demographic visibility preferences

08. Subscribing organizations

Subscribing organizations are bound by additional data handling requirements through the ethical use agreement.

8.1 What subscribers can do with content

- Access anonymized published content within their subscription tier
- Use content for the purposes stated in their application (staff training, program design, policy work)
- Save content to their internal systems for the duration of their subscription
- Discuss content within their organization

8.2 What subscribers cannot do

- Redistribute content externally
- Share account credentials
- Attempt to identify contributors
- Use content in commercial contexts beyond their subscription scope without renewed consent
- Use content in ways that conflict with MindBank values

8.3 Subscriber security expectations

Subscribing organizations must:

- Maintain reasonable information security in their handling of accessed content
- Limit internal access to staff who need it for the stated purposes
- Notify MindBank within 5 business days of any actual or suspected breach affecting their subscriber data or accessed content
- Allow audit on reasonable request

8.4 Subscriber breach implications

If a subscribing organization breaches the ethical use agreement or fails to maintain reasonable security:

- Access is suspended pending investigation
- Affected contributors are notified
- Confirmed breaches result in subscription termination
- Pattern of poor practice may be publicly disclosed in transparency reports

09. Annual review and continuous improvement

9.1 Annual security review

Each year, the Privacy Officer conducts a full review covering:

- All access lists and permissions
- All vendor relationships and their continued compliance
- Recent incidents and the effectiveness of our response
- Gaps identified in the past year
- Updates needed to this policy
- External threat landscape changes
- Findings published in the annual transparency report (without identifying details)

9.2 Independent review

Every two years, MindBank engages an independent reviewer (security consultant or auditor) to assess our practices. The first independent review is planned for Year 2 of the pilot.

Findings from independent reviews are addressed within 6 months and reported on publicly.

9.3 Threat-informed updates

When new threats emerge in our sector (e.g., new attack vectors against nonprofits, new privacy regulations, new vendor incidents), this policy is updated within 30 days. The change log records what changed and why.

10. Limits of this policy

10.1 Things this policy doesn't cover

- **Legal advice.** This policy describes our practices. Legal questions about specific situations should go to qualified counsel.
- **Contributor agreements.** The binding terms with individual contributors are in the contributor agreement, not here.
- **Subscriber agreements.** The binding terms with subscribing organizations are in the ethical use agreement, not here.
- **Cybersecurity in absolute terms.** We commit to strong, reasonable, and continuously-improved protections. We do not promise that no incident will ever occur.

10.2 Where this policy must give way

If this policy ever conflicts with:

- **Canadian law** (PIPEDA, provincial privacy law, etc.) — the law governs
- **A specific contributor's revoked consent** — the consent revocation governs
- **Our published Privacy Policy** — the Privacy Policy commitment governs (we promised more, we deliver more)

If you find such a conflict, escalate to the Privacy Officer immediately.

11. Updating this policy

This policy is reviewed:

- **Annually** as part of the security review
- **Within 30 days** of any incident that reveals a gap
- **Whenever technical infrastructure changes** materially (new database, new hosting, new payment processor)
- **Whenever the regulatory environment changes**

Updates require Privacy Officer approval. Material updates are communicated to all persons with system access within 14 days of approval.

Change log

- April 2026 — Version 1.0: Initial policy.

A. Appendix A — Access matrix

(Placeholder for the detailed access matrix document. To be developed alongside platform technical architecture. Lists each role × each data category × authorized actions.)

B. Appendix B — Vendor inventory

(Placeholder for the vendor inventory. Lists each vendor, the data they process, the DPA on file, and the date of last review.)

A NOTE FROM THE PRIVACY OFFICER

Promises *we can keep.*

A data protection policy is a promise that the systems and people behind it can keep. This document represents the promises I'm willing to make on MindBank's behalf — and the operational discipline I'm committing to maintain.

If you are reviewing this as a funder, partner, or auditor and find that any commitment here is not matched by what you observe in practice, that is a serious finding and I want to hear about it directly.

> *Privacy and security are not one-time achievements. They are practices that have to be renewed every day, with every decision about how data flows through the systems we build.*

— Stephanie Atwood, Privacy Officer