exposurebureau.com

exposure bureau

DIGITAL-RISK QUANTIFICATION

PUBLIC

Information Security Whitepaper

Security, privacy, and operational controls Exposure Bureau implements to protect client information and the data products derived from licensed and public sources.

DOCUMENT DOC 02 VERSION v2.0 DATE 2026-05-23 ENTITY Exposure Bureau LLC

This whitepaper describes the security and privacy controls Exposure Bureau (operated by Exposure Bureau LLC, a US limited liability company) implements to protect the confidentiality, integrity, and availability of client information and the data products derived from public and licensed sources.

1 Purpose

It is intended for:

- Prospective and active clients conducting vendor security assessments;
- Clients' internal security, privacy, and procurement teams;
- Auditors operating under NDA on behalf of clients;
- Underwriters of clients' cyber-liability or E&O policies who may review vendor controls.

This document is not a SOC 2 report. Exposure Bureau intends to pursue SOC 2 Type I in the twelve (12) months following its first commercial revenue and SOC 2 Type II thereafter. This whitepaper describes the controls that will be evaluated under that audit.

2 About Exposure Bureau

Exposure Bureau produces decision-grade digital-risk exposure indices from public and licensed sources. The corpus is assembled from licensed data partners (Have I Been Pwned, DarkOwl Vision, SpyCloud, Constella Intelligence, Flare, Webz.io) and public, indexed sources: ransomware leak-site metadata, initial-access-broker listings, paste sites, public Telegram channels, internet-wide scanners, certificate-transparency logs, and regulator disclosures (HHS / SEC / state AG / FTC).

The primary product is a **recurring intelligence report** (weekly or monthly PDF + executive email digest). Exposure Bureau also delivers one-shot M&A and vendor diligence reports, signed evidence packages, and API access (roadmap; Mandate / MSSP tier). It is report-first, not a self-serve dashboard.

Exposure Bureau does not offer offensive-security services, penetration testing, take-down execution, threat-actor engagement, or any service that requires authentication bypass on third-party systems. Every collection method is either (a) observation of public data sources, or (b) consumption of data made available under a current commercial license from a named provider.

3 Governance and roles

ROLE	RESPONSIBILITIES
Founder / CEO	Ultimate owner of the security and privacy program.
Security Lead (acting: Founder)	Owns the controls described in this document; reviews quarterly.
Privacy Officer (acting: Founder)	Owns data-subject-rights handling, DPIA, and lawful-basis review.

ROLE	RESPONSIBILITIES
Engineering	Implements technical controls; conducts code review.
External Counsel	Reviews contracts, data flows, and incident response; on retainer.
External Auditor (future)	Performs SOC 2 examinations and penetration tests.

Until Exposure Bureau's headcount reaches a size that makes role separation operationally meaningful (estimated 6+ FTEs), the Founder holds the Security Lead and Privacy Officer roles concurrently. This concentration is disclosed; client review is expected during procurement. The security program is reviewed at least annually and after any material change in service, infrastructure, or applicable law.

4 Asset management

4.1 Asset inventory

Exposure Bureau maintains an up-to-date inventory of:

- **Information assets:** client-supplied data (engagement configuration, declared domains/brands/vendors, SBOMs), Exposure-Bureau-owned datasets (signal records, computed indices, derived metrics), and operational data (logs, telemetry).
- **Software assets:** production code repositories, infrastructure-as-code definitions, third-party libraries and their pinned versions.
- **Hardware assets:** managed cloud accounts (Cloudflare, Supabase) and self-managed virtual servers hosting collector workloads. No physical assets are operated by Exposure Bureau.

Assets are classified by sensitivity:

CLASS	DESCRIPTION	EXAMPLES
Public	May be disclosed freely.	Marketing materials, the methodology whitepaper, this whitepaper.
Internal	Operational data; default class.	Internal runbooks, source-list configurations.
Confidential	Client-derived or client-identifying.	Engagement configuration, computed indices, client contacts.
Restricted	High-impact secrets and PII.	Signing keys, API credentials, plaintext PII pending redaction, per-tenant salts.

4.2 Data flow

Client data and externally-collected data are processed in segregated logical pipelines. Client-supplied configuration is uploaded over TLS, stored in a tenant-isolated Postgres schema, and exposed only via authenticated APIs subject to row-level security (RLS).

Externally-collected data is ingested by isolated collector processes (Section 7.2), normalized, hashed where it contains PII, and stored in Exposure-Bureau-controlled schemas with no inbound client access except through derived indices.

5 Access control

5.1 Identity

Client access to the Exposure Bureau application is authenticated via Supabase Auth using one or more of: passwordless email magic links, single sign-on (SSO) via the client's IdP (Mandate tier), and OAuth providers where contractually agreed. Multi-factor authentication (MFA) using TOTP is mandatory for all administrative and Mandate-tier user accounts.

Internal access to production infrastructure is authenticated via the operating provider's IdP (Supabase, Cloudflare, GitHub) and requires hardware-backed MFA (FIDO2 / WebAuthn) for the founder and any future engineering staff.

5.2 Authorization

All client-facing data tables enforce Postgres row-level security keyed on tenant identifier. Internal collector and admin tables are not exposed to any client-facing JWT. Service accounts used by collectors and Edge Functions use Supabase service-role credentials with table-level grants scoped to the minimum necessary, rotated quarterly or upon staff change.

5.3 Privileged access

Privileged operations — production database migrations, secret rotations, client data deletion — require dual control where personnel allow. While Exposure Bureau operates with a single founder, dual control is approximated by automated peer review (every change is committed to a Git repository, signed, and CI-validated; emergency runbook deviations are logged with after-the-fact review).

5.4 Joiner / mover / leaver

A documented JML procedure governs onboarding, role-change, and offboarding events. Off-boarding triggers immediate revocation of all production credentials, rotation of any shared secrets touched, and an access-review attestation. While Exposure Bureau has no employees other than the founder, the procedure is in place for future hires and contractors.

6 Cryptography

6.1 Encryption in transit

All HTTP traffic to client-facing endpoints is served exclusively over TLS 1.2 or higher, with TLS 1.3 preferred. HSTS is enabled with `max-age=31536000; includeSubDomains; preload`. Cipher suites and certificates are reviewed twice per year against the latest Mozilla recommendations. Internal traffic between collectors and

Supabase, and between Edge Functions and Supabase, occurs over TLS-encrypted Postgres connections (`sslmode=verify-full`).

6.2 Encryption at rest

Client data and Exposure-Bureau-managed data stored in Supabase Postgres are encrypted at rest using AES-256 (Supabase-managed encryption). Object storage (PDF reports, evidence packages) is encrypted at rest in Supabase Storage. Collector-host filesystems are LUKS-encrypted; collectors persist no client-identifying data to disk by default.

6.3 Hashing of PII

Identifiers observed in any pipeline (stealer logs, breach feeds, public posts) are hashed at ingest using SHA-256 with a per-tenant rotating salt. Salts rotate quarterly (and on demand following a security incident). We store only the hash plus observation metadata. Plaintext is retained no longer than thirty (30) days and only when required for client-side notification obligations under applicable law (e.g., GDPR Art. 34); plaintext dereferencing requires verified domain ownership and a documented lawful basis. First-party leads (waitlist, resource requests) are consent-based and stored as given.

6.4 Signing keys

Evidence packages are signed with an Ed25519 keypair held in a hardware-backed key store. The public key is published at `https://exposurebureau.com/.well-known/evidence-pubkey.txt` so any party may verify a signature without contacting Exposure Bureau. Key rotation occurs annually with an overlap window during which both old and new public keys are published.

6.5 Secrets management

Production secrets (API keys, salts, signing keys) are stored in the secret stores native to each provider (Supabase Vault, Cloudflare secrets / environment bindings) and never committed to source control. Pre-commit hooks and CI scan for credential patterns. Discovered credentials are rotated immediately and the discovery is logged.

7 Operations security

7.1 Production architecture

- **Frontend:** Next.js (App Router) on Cloudflare Pages (via `@cloudflare/next-on-pages`); API routes run on the edge runtime.
- **API and database:** Supabase (Postgres, Auth, Storage, Edge Functions).
- **Rate limiting:** Cloudflare KV.
- **Collectors:** isolated processes on virtual servers, geographically distributed across at least two regions.
- **PDF generation:** headless rendering on a dedicated host.
- **Email delivery:** a reputable transactional provider (Resend or equivalent).
- **Observability:** structured logs, metrics, and error tracking via managed providers.

- **Source control and CI:** GitHub.

A single-region failure of either Cloudflare or Supabase results in service degradation; both providers operate multi-region for their respective services on Exposure Bureau's plans.

7.2 Isolation

Each collector class (licensed feeds, leak-site metadata, IAB listings, paste/forum/Telegram, internet-wide scanning, threat-intel feeds, regulatory portals) runs as an isolated process with its own credentials, its own egress network controls, and no shared state at the operating-system level. A compromise of one collector does not by design grant access to another collector's credentials, to client data, or to the Supabase service-role secret.

7.3 Logging and monitoring

All production services emit structured logs. Logs are retained for at least one (1) year in hot storage and longer in cold storage where required by contractual or regulatory obligation. Logs do not contain plaintext credentials, full PII, or signing-key material. Metrics covering request latency, error rate, queue depth, collector throughput, and pipeline lag are visible on internal dashboards; alerts are routed to the on-call rotation (currently: founder).

7.4 Change management

All production changes are introduced through pull requests against the main branch. CI runs typing, linting, unit tests, and dependency vulnerability scans. Merges to main trigger automatic deployment to a staging environment; production deployment requires explicit promotion. Database schema changes are introduced through versioned migrations applied via Supabase's migration tooling, run against staging first and then against production with an explicit confirmation step.

7.5 Backups

Supabase performs daily encrypted backups of the production database with point-in-time recovery (PITR) over the trailing seven (7) days. Backups are retained for thirty (30) days. Backup restoration is tested quarterly.

7.6 Vulnerability management

Third-party dependencies are scanned by GitHub Dependabot and `npm audit` in CI. Critical and high-severity vulnerabilities are patched within seven (7) and thirty (30) days respectively, where a patch is available; when none exists, mitigations are documented and tracked to resolution. Infrastructure components are updated monthly or upon a critical CVE, whichever is sooner; automated reboots for kernel security patches are enabled.

8 Communications security

8.1 Network

Client-facing services are reachable only via TLS on port 443. Collectors initiate outbound connections to Supabase, to source endpoints, and to monitoring services; inbound connections to collectors are restricted to administrative SSH from a small allowlist of operator IP ranges with key-only authentication and Fail2ban.

8.2 Email

Email originating from Exposure Bureau domains is sent through SPF-, DKIM-, and DMARC-aligned configurations with a strict `p=reject` DMARC policy. Inbound email is routed through a hosted provider with spam and phishing filtering enabled.

9 System acquisition, development, and maintenance

9.1 Secure development lifecycle

All production code is held in a private GitHub repository. Commits are signed where supported. Pull requests require at least one reviewer; in the single-founder phase, the founder reviews changes against a documented checklist that includes security implications. STRIDE-based threat modeling is performed for each new feature that introduces a new data flow, authentication surface, or third-party integration, and is committed alongside the feature.

9.2 Third-party libraries

Production runtime dependencies are pinned by version and hash. New dependencies undergo a lightweight review (publisher reputation, maintenance status, license compatibility) before adoption. License inventory is reviewed annually.

9.3 Penetration testing

Exposure Bureau will commission an annual external penetration test by a reputable third party once it exceeds 25 active paying clients or once it pursues SOC 2 Type I, whichever occurs first. Findings are tracked to resolution; an executive summary is made available to clients under NDA.

10 Supplier and sub-processor management

10.1 Selection

Suppliers handling client data or Exposure-Bureau-confidential data are selected based on (a) security and privacy posture, including their own attestations (SOC 2, ISO 27001, or equivalent), (b) data-residency and transfer mechanisms, and (c) contractual willingness to enter into a Data Processing Agreement with adequate sub-processor and incident terms.

10.2 Sub-processor list

The current list of sub-processors is maintained as a separate document and published at `https://exposurebureau.com/trust/subprocessors`. Sub-processors include infrastructure providers (Supabase, Cloudflare), email delivery (Resend or equivalent), observability providers, and the licensed data partners that supply collection feeds (Have I Been Pwned, DarkOwl, SpyCloud, Constella, Flare, Webz.io). Clients are notified in writing of any change at least fifteen (15) days before it takes effect, with a right to object on material grounds.

> COUNSEL REVIEW
> The contractual sub-processor change-notice period (15 days), the right-to-object mechanism, and whether each named licensed data partner is correctly characterized as a sub-processor vs. an independent controller/source provider should be confirmed by counsel against the DPA and each partner's data-license terms.

10.3 Ongoing oversight

Each sub-processor's continued use is reviewed at least annually. Material incidents (sub-processor breaches, changes of control) trigger an interim review.

11 Information security incident management

11.1 Incident definition

An incident is any event that has, or is reasonably suspected to have, caused (a) unauthorized access to or disclosure of client data or Exposure-Bureau-confidential data, (b) unauthorized modification of indices or reports, (c) extended service unavailability, or (d) violation of Exposure Bureau's stated source-collection limits.

11.2 Response

The incident response plan is documented separately. Summary lifecycle:

1. **Detection** — via monitoring, client report, sub-processor notification, or external researcher disclosure.
2. **Triage** — incident lead (Founder / Security Lead) classifies severity (P0–P3) within one (1) hour of detection.
3. **Containment** — immediate action to stop the bleeding; documented and timestamped.
4. **Eradication** — root cause identified and removed.
5. **Recovery** — service restored; integrity validated.
6. **Notification** — affected clients notified without undue delay and in any case within seventy-two (72) hours for incidents reasonably likely to affect them; regulatory notifications made as required by applicable law.
7. **Post-mortem** — within fifteen (15) business days, a written post-mortem is produced and shared with affected clients.

> COUNSEL REVIEW
> The 72-hour client-notification commitment and the carve-out for "incidents reasonably likely to affect them" should be reconciled by counsel with the breach-notification timelines in the MSA/DPA and with statutory deadlines (GDPR Art. 33/34, US state breach laws) to ensure the contractual promise is not narrower or broader than the legal obligation.

11.3 Client cooperation

Exposure Bureau cooperates in good faith with affected clients' own incident response, including providing forensic data, indicators, and timelines, subject to the protection of other clients' data and Exposure Bureau's legal obligations.

11.4 Disclosure to researchers

Exposure Bureau operates a coordinated disclosure policy. Researchers may report vulnerabilities to security@exposurebureau.com or via a published `.well-known/security.txt`. Exposure Bureau commits to acknowledging reports within seventy-two (72) hours and to good-faith handling. No legal action will be taken against researchers acting in good faith and within the scope of the disclosure policy.

12 Business continuity and disaster recovery

12.1 Service tier

Exposure Bureau's contractual availability target (SLA) is 99.5% calculated monthly for client-facing endpoints, with separate availability targets for asynchronous deliverables (recurring reports, board decks, alerts) specified in the SLA document.

12.2 Recovery objectives

- **Recovery Time Objective (RTO):** twenty-four (24) hours for client-facing service restoration from a complete provider outage.
- **Recovery Point Objective (RPO):** twenty-four (24) hours for non-real-time data; one (1) hour for the most recent computed indices, supported by Supabase point-in-time recovery.

12.3 Provider redundancy

Where service-tier and cost allow, Exposure Bureau maintains exportable representations of critical data (computed indices, configuration, client inputs) that could be restored against an alternate provider in the event of prolonged Supabase or Cloudflare unavailability. This is a degraded-mode fallback, not a hot standby.

12.4 Tabletop exercises

Disaster-recovery scenarios are exercised at least annually. Findings inform the BCP and IRP.

13 Privacy and compliance

13.1 Applicable regimes

Exposure Bureau operates as a service provider serving clients globally. The following regimes are relevant by default:

- **United States** — CCPA/CPRA, Virginia CDPA, Colorado CPA, Connecticut CTDPA, and other state laws as they enter effect.
- **European Union and EEA** — GDPR, with Standard Contractual Clauses (2021/914) for cross-border transfers.
- **United Kingdom** — UK GDPR with the International Data Transfer Addendum (IDTA).
- **Brazil** — Lei Geral de Proteção de Dados (LGPD).
- **Japan** — Act on the Protection of Personal Information (APPI).

- **Australia, Singapore, Canada (PIPEDA)** — handled by contract where clients are present in those jurisdictions.

> COUNSEL REVIEW
>
> The roster of named privacy regimes, the chosen transfer mechanisms (SCCs 2021/914, UK IDTA), and the controller/processor characterization in Section 13.2 should be confirmed by counsel for the jurisdictions Exposure Bureau actually serves at launch, and updated as new US state laws take effect.

13.2 Roles

In the client relationship, the client is the controller and Exposure Bureau is the processor. For Exposure Bureau's own corporate processing (employees, suppliers) and for first-party leads collected on consent, Exposure Bureau is the controller.

13.3 Data minimization

Exposure Bureau applies the principle of data minimization at ingest. Plaintext personal identifiers from external sources are hashed at ingest with rare, time-bound exceptions (Section 6.3). Default retention for collected signals is thirteen (13) months, configurable per category; first-party leads are retained until a deletion request.

13.4 Data subject rights

Requests under GDPR Articles 15–22, CCPA §1798.105–130, LGPD Articles 17–22, and equivalent provisions are handled per the Data Retention & Deletion Policy. Requests directed at the client's data are forwarded to the client; requests directed at Exposure Bureau's own controller-mode processing are handled by Exposure Bureau. A first-party deletion path exists: `POST /api/privacy/delete`.

> COUNSEL REVIEW
>
> The specific data-subject-rights articles cited and the division of responsibility between controller (client) and processor (Exposure Bureau) for fulfilling requests against hashed third-party identifiers should be verified by counsel, particularly the lawful basis for processing scraped third-party PII and the adequacy of the hashing-as-minimization argument.

13.5 CSAM handling

Any content classified as Child Sexual Abuse Material at ingest is immediately discarded from indices and from raw storage. Only the infohash plus detection timestamp is retained for the purpose of reporting to the National Center for Missing & Exploited Children (NCMEC) or equivalent bodies in the applicable jurisdiction. The detailed procedure is documented in the CSAM Detection & Reporting SOP, available to clients and regulators on request.

13.6 Personnel security

All personnel with access to production systems sign a Confidentiality and Acceptable Use agreement. Background checks are performed for any future hires whose role requires direct production access, to the extent permitted by the applicable jurisdiction.

14 Acceptable use of Exposure Bureau outputs by clients

Exposure Bureau outputs are intended for defensive, due-diligence, brand-protection, and risk-quantification use cases. The contractual prohibitions on client use are specified in the Acceptable Use Policy. Examples of prohibited client use include offensive-security campaigns against third parties, contact or harassment of individuals identified in indices, and resale of raw Exposure-Bureau-derived data without written authorization.

15 Compliance roadmap

MILESTONE	TARGET
Documented IR and BCP procedures with annual tabletop	Within 6 months of first paying client
External penetration test	Within 12 months or 25 active clients, whichever is first
SOC 2 Type I readiness assessment	Within 12 months of first paying client
SOC 2 Type I report	Within 18 months of first paying client
SOC 2 Type II report	12 months after Type I
ISO 27001 (if client demand justifies)	Decision point after SOC 2 Type II

16 Contact

- Security and vulnerability reports: security@exposurebureau.com
- Privacy inquiries, DSARs, contract, procurement, and methodology questions: hello@exposurebureau.com

End of document. Information Security Whitepaper version 2.0 — 2026-05-23. Exposure Bureau LLC, exposurebureau.com.