ThreatShield AI – Privacy Policy

Last updated: September 26, 2026

This Privacy Policy explains how **NortAvex Inc.** (“NortAvex,” “we,” “us,” or “our”) collects, uses, discloses, and protects information in connection with the ThreatShield AI platform (the “Platform”). It applies to Customers, Authorized Users, and visitors to our marketing site, and should be read together with our Terms and Conditions.

For clarity: much of the security-related content processed by the Platform (e.g., alerts, logs, indicators of compromise) originates from Customer's own connected systems. For that content, Customer acts as the data controller and NortAvex acts as a data processor / service provider acting on Customer's behalf — see Section 10.

1. Information We Collect

- **Account & registration data** — name, work email address, organization name, role, and authentication credentials (passwords are stored as salted hashes, never in plain text).
- **Usage & device data** — IP address, browser/device information, login timestamps, session activity, and general usage patterns within the Platform.
- **Customer Security Data** — security alerts, incidents, logs, indicators of compromise, and related metadata that Customer connects to or uploads into the Platform via SIEM integrations (e.g., Wazuh, Elastic, Splunk, Microsoft Sentinel) or manual entry. This may incidentally include personal information about Customer's own personnel or end users (e.g., usernames or IP addresses appearing in log data) that Customer's own systems generate.
- **SIEM integration credentials** — connection credentials Customer provides to link a third-party security tool; these are encrypted at rest and destroyed immediately upon organization deletion.
- **Billing information** — billing contact details and subscription/plan information. Full payment card data is collected and processed directly by our payment processor, Stripe; we do not store complete card numbers.
- **Uploaded files** — organization logo images, if uploaded.
- **Support communications** — information provided when contacting support.
- **Audit & security logs** — records of actions taken within the Platform (who did what, when), retained for security, accountability, and compliance purposes.

2. How We Use Information

We use the information described above to: (a) provide, operate, and maintain the Platform, including AI-assisted alert triage and threat-intelligence enrichment; (b) authenticate users and secure accounts; (c) process billing and manage subscriptions; (d) provide customer support; (e) maintain audit trails and investigate misuse or security incidents; (f) comply with legal obligations; and (g) improve the Platform's features and reliability. We do not use Customer Data to train third-party AI models beyond what is disclosed in Section 3, and we do not sell personal information.

3. AI Processing of Data

- The Platform uses AI models, currently provided by **Anthropic**, to generate alert summaries, investigative findings, and recommendations. Relevant alert content is sent to this provider's API for processing in order to generate that output.
- Under our current arrangement, data submitted through the API is not used to train the provider's underlying models, consistent with their commercial API data-use terms.
- AI Output does not itself set risk or priority scores — those are computed by NortAvex's own deterministic logic — and does not autonomously adjudicate, close, or take action on alerts without human review.
- When enabled, prompt and response content may also be sent to **LangSmith**, a third-party AI-observability service, to help us debug and monitor AI output quality. See Section 6.

4. Legal Basis for Processing (Where GDPR Applies)

Where the GDPR applies, we process personal information on the following bases: performance of a contract (providing the Platform to Customer); our legitimate interests (securing the Platform, preventing fraud, improving the Service); compliance with legal obligations; and, where required, consent.

5. Data Sharing — We Do Not Sell Personal Information

We do not sell personal information. We share information only as described in this Policy or as required by law.

6. Sub-processors

We use the following categories of third-party sub-processors to operate the Platform:

Sub-processor	Purpose	Data involved
Amazon Web Services (AWS)	Cloud hosting infrastructure (Canada — ca-central-1 region)	All Platform data
Anthropic	AI-assisted alert analysis and recommendations	Alert content submitted for AI processing
Stripe	Payment processing	Billing contact and payment information
Resend	Transactional email delivery (notifications, password resets)	Name, email address
LangSmith (LangChain)	AI observability / debugging of AI output quality, when tracing is enabled	AI prompt and response content

We may update this list as our vendors change; material changes affecting the processing of personal information will be reflected in an updated version of this Policy.

Separately, the Platform enriches Customer's alerts using external threat-intelligence sources (including CIRCL, Botvrij.eu, Emerging Threats, Blocklist.de, AbuseIPDB, abuse.ch/Spamhaus, CISA KEV, EPSS, MITRE ATT&CK, and SigmaHQ). These sources provide data *into* the Platform to enrich alerts — they are not sent Customer Data.

7. International Data Transfers

Our primary infrastructure is hosted in Canada. Certain sub-processors (including our AI provider) may process data in the United States or other jurisdictions. Where we transfer personal information internationally, we rely on appropriate safeguards required by applicable law, such as contractual protections with our sub-processors.

8. Data Retention

Data type	Retention
Operational data (incidents, alerts, uploaded files, comments)	Soft-deleted, then permanently deleted after 90 days
User profiles	Soft-deleted, then anonymized after 90 days
Organization (tenant) profiles	Soft-deleted, then anonymized after 90 days
Audit logs	Retained independently for 12 months (standard plans) or 24 months (enterprise plans) from organization deletion
Billing / payment records	Retained for a minimum of 7 years, as required for tax and legal purposes
SIEM integration credentials	Destroyed immediately upon organization deletion

9. Your Rights

Subject to applicable law (including Law 25 and, where applicable, GDPR), you may have the right to: request access to personal information we hold about you; request correction of inaccurate information; request deletion or anonymization of your account; request a copy of your information in a portable format; object to or restrict certain processing; and withdraw consent where processing is based on consent. To exercise these rights, send a written request to our Privacy Officer at **privacy@nortavex.com** (see Section 17); account-specific requests may also be sent to **support@threat-shield.ai**. We may need to verify your identity before acting on a request, and we will respond in writing within 30 days of receiving it. If you are not satisfied with our response, you may have the right to lodge a complaint with the applicable data protection authority (in Quebec, the Commission d'accès à l'information).

10. Your Role as Controller of Customer Security Data

For Customer Security Data that Customer connects to the Platform from its own environment (e.g., via SIEM integrations), Customer is the data controller and determines what data is submitted, including any personal information about Customer's own personnel contained in that data. NortAvex processes that data as a service provider on Customer's instructions, as further described in the applicable customer agreement.

11. Account Deletion

Authorized Users may request deletion of their account, and organization administrators may request deletion of the organization, through the Platform. Requests are subject to an approval and retention process described in Section 8. Where legally required (e.g., a request framed as a right to erasure),

applicable personal information is anonymized immediately upon approval rather than after the standard retention window.

12. Cookies & Similar Technologies

The Platform uses strictly necessary cookies for authentication and session management (HTTP-only, secure, same-site protected). We do not currently use third-party advertising or analytics tracking cookies. If this changes, we will update this Policy and provide any consent mechanism required by applicable law.

13. Data Security

We apply administrative, technical, and physical safeguards designed to protect information, including encryption in transit, encryption of sensitive credentials at rest, role-based access controls, append-only audit logging, network isolation of production systems, and restricted, consent-based support access to customer accounts. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

14. Data Breach Notification

In the event of a confirmed security incident involving personal information, we will notify affected Customers and, where required by applicable law (including Law 25 and GDPR), the relevant supervisory authority, without undue delay and in accordance with applicable legal timelines.

15. Children's Privacy

The Platform is a business (B2B) product intended for use by authorized professional personnel. It is not directed at, and we do not knowingly collect personal information from, individuals under the age of 18.

16. Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be communicated via the Platform or by email before taking effect. The “Last updated” date above reflects the most recent revision.

17. Quebec Law 25 — Privacy Officer

As required by the Act respecting the protection of personal information in the private sector (Quebec, “Law 25”), NortAvex has designated the following person as responsible for the protection of personal information (our “Privacy Officer”):

Juliette Cyr
Vice President / Privacy Officer
NortAvex Inc.
Email: privacy@nortavex.com
Mailing address: 102 Rue de Touraine, Lévis, Quebec G6J 2A8, Canada

The Privacy Officer oversees NortAvex's compliance with Law 25, including responding to requests to access or correct personal information and handling complaints about how we process personal information. Requests and complaints should be submitted in writing to the contact details above.

18. Governing Law

This Privacy Policy is governed by the laws of the Province of Quebec and the applicable federal laws of Canada. This does not limit any rights you may have under mandatory data protection laws that apply to you, such as the GDPR.

19. Contact Us

Questions or requests regarding this Privacy Policy may be directed to:
NortAvex Inc.
Privacy Officer (Juliette Cyr): privacy@nortavex.com
General inquiries: info@threat-shield.ai
Support requests: support@threat-shield.ai
Address: 102 Rue de Touraine, Lévis, Quebec G6J 2A8, Canada

This document was prepared based on a review of the ThreatShield AI platform's actual data flows, sub-processors, and retention configuration as of September 2026. It is provided as a working draft and is **not legal advice.** It should be reviewed by NortAvex's legal counsel — including the French-language version expected for Quebec users under the Charter of the French Language — before publication.