

FlightHorizon ALERT Privacy Policy

Effective Date: May 21, 2026

Last Updated: May 21, 2026

This Privacy Policy describes how Vigilant Aerospace Systems, Inc. (“Company,” “we,” “us,” or “our”) collects, uses, discloses, retains, and protects personal information in connection with FlightHorizon ALERT and related services, features, data, Documentation, support, hardware, and websites or pages that link to this Privacy Policy (collectively, the “Services”).

Capitalized terms not defined in this Privacy Policy have the meanings given to them in the FlightHorizon ALERT Subscription Terms of Service or the applicable Order Form.

1. Scope and Relationship to the Terms.

- a.** This Privacy Policy applies to personal information processed by Company in connection with the Services. “Personal information” means information that identifies, relates to, describes, or can reasonably be linked to an identified or identifiable natural person.
- b.** This Privacy Policy does not replace the applicable Terms, Order Form, confidentiality obligations, data rights, or other written agreement between Company and Customer. If Customer submits Customer Data that includes personal information, Customer is responsible for having the authority, notices, consents, and rights necessary for Company to process such information in connection with the Services.
- c.** The Services are intended for business and operational use by Customers and Authorized Users, not for personal, household, or consumer use.

2. Information We Collect.

- a. Account and Contact Information.** We may collect names, business contact details, company name, job title, account identifiers, account settings, notification preferences, and other information provided to create, administer, or support a Customer account or Authorized User account.
- b. Authorized User and Credential Information.** We may collect information associated with Account Credentials, authentication, access permissions, account status, login activity, and administrative actions. Passwords and other credentials should be protected by Customer and Authorized Users in accordance with the Terms.
- c. Customer Data.** We may collect, store, access, and process Customer Data submitted, uploaded, entered, transmitted, imported, or otherwise made available by Customer or Authorized Users through or in connection with the Services, including operational settings, notes, records, preferences, and other information used to configure or operate the Services.
- d. Receiver, Hardware, and Operational Data.** Where a Receiver or other Hardware is provided or used, we may collect ADS-B Data, Remote ID Data, other data received or transmitted by the Receiver, hardware status, diagnostic information, connectivity information, installation or configuration information, receiver location or deployment information when provided or required for operation, and related operational logs.
- e. Usage Data and Device Information.** We may collect Usage Data and technical information about use of the Services, including log data, feature usage, pages or screens viewed, export activity, alerts generated or delivered, timestamps, IP address, browser or device type, operating system, approximate location derived from network information, performance data, error reports, and security or audit logs.
- f. Communications and Support Information.** We may collect information contained in communications with Company, including emails, text messages, support requests, call

notes, forms, feedback, and records of operational, legal, billing, account, and alerting notifications.

g. Subscription, Trial, Billing, and Payment Information. We may collect subscription status, Trial Access information, billing contact information, invoices, payment status, transaction records, and related account information. Payment information may be processed by Company or by payment processors acting on Company's behalf.

h. Cookies and Similar Technologies. We may use cookies, pixels, local storage, log files, analytics tools, and similar technologies to operate, secure, analyze, and improve the Services and related websites or pages.

3. How We Use Information.

a. To provide, operate, maintain, administer, and support the Services, including account administration, authentication, access control, data processing, alerting, notification delivery, Receiver or Hardware operation, support, troubleshooting, and customer service.

b. To manage Subscriptions, Trial Access, billing, payments, renewals, account records, Order Forms, and contractual relationships with Customers.

c. To send operational notices, alerting notifications, service-related notices, account information, billing notices, legal notices, support communications, security notices, and other communications related to the Services.

d. To monitor, inspect, audit, secure, and protect the Services, accounts, systems, networks, data, and users; to detect, prevent, investigate, and respond to outages, security incidents, unauthorized access, fraud, abuse, policy violations, and other harmful activity; and to enforce the Terms and applicable Order Forms.

e. To analyze usage and performance, improve and train the Services, develop new features or offerings, maintain competitiveness, conduct statistical analysis, and create aggregated, anonymized, or de-identified information that does not identify Customer, Authorized Users, or any other natural person.

f. To comply with applicable law, regulations, legal process, court orders, governmental requests, export-control obligations, recordkeeping obligations, and contractual obligations.

g. To protect the rights, safety, security, property, and interests of Company, Customers, Authorized Users, service providers, affiliates, and others.

h. For other purposes with Customer's or the applicable individual's consent, or as otherwise described at the time information is collected.

4. Communications; Email and Text Notifications.

a. By providing an email address and/or mobile phone number and using the Services, Customer and Authorized Users authorize Company to send electronic communications, including email and, where applicable, text messages (SMS), using contact information associated with the account and notification settings within the Services.

b. Communications may include operational notices, alerting notifications, service-related notices, account information, billing notices, legal notices, support communications, security communications, and other information related to the Services. Message and data rates may apply to SMS messages, and message frequency may vary.

c. Customer and Authorized Users may modify notification preferences, disable email or SMS notifications, or otherwise turn off available notifications through settings made available within the Services, by following the instructions in the applicable

communication, by replying as directed in an SMS message, or by contacting Company. Disabling or limiting operational or alerting notifications may reduce the functionality of the Services or the ability to receive timely alerts, warnings, or other operational information.

- d. Nothing in this Privacy Policy limits Company's ability to send non-marketing legal, security, account, billing, or other administrative communications necessary to provide or administer the Services.

5. How We Disclose Information.

- a. **Affiliates and Personnel.** We may disclose information to Company affiliates and to Company personnel who need the information to perform their duties or support the Services.
- b. **Service Providers and Subcontractors.** We may disclose information to vendors, contractors, consultants, payment processors, hosting providers, communications providers, analytics providers, support providers, professional advisers, and other service providers that assist with the Services, subject to appropriate confidentiality and use restrictions.
- c. **Customer and Account Administrators.** We may disclose information to the Customer, account administrators, and Authorized Users as necessary to provide, administer, support, or secure the Services or to respond to Customer instructions and requests.
- d. **Legal, Safety, and Compliance.** We may disclose communications, records, Customer Data, Usage Data, account information, and other information to the extent required or permitted by law, legal process, court order, governmental request, export-control requirements, or to protect the rights, safety, security, property, or interests of Company, Customers, Authorized Users, service providers, affiliates, or others.
- e. **Business Transactions.** We may disclose information in connection with a merger, acquisition, financing, reorganization, sale of assets, bankruptcy, receivership, or similar corporate transaction involving Company or a portion of its business.
- f. **With Consent or Direction.** We may disclose information with Customer's or the applicable individual's consent or direction, including when Customer enables integrations, shares reports, authorizes publication, or requests support.
- g. **Aggregated or De-Identified Information.** We may use and disclose aggregated, anonymized, or de-identified information for business, commercial, analytical, product development, training, benchmarking, marketing, or other lawful purposes, provided such information does not identify Customer, Authorized Users, or any other natural person.

6. Customer Responsibilities.

- a. Customer is responsible for the legality, accuracy, quality, and appropriateness of Customer Data and for providing all required notices and obtaining all required consents, authorizations, rights, and permissions from Authorized Users and other individuals whose personal information is submitted to or processed through the Services.
- b. Customer is responsible for configuring the Services, managing Authorized Users, maintaining accurate account contact information, and using commercially reasonable security measures to protect information transmitted to or from Customer through or in connection with the Services.
- c. Customer should not submit sensitive personal information, regulated personal information, or information about third parties unless Customer has determined that such submission is lawful, necessary, and authorized for Customer's use of the Services.

7. Data Security.

- a.** Company uses reasonable administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, use, disclosure, alteration, or destruction. No method of transmission over the internet or electronic storage is completely secure, and Company cannot guarantee absolute security.
- b.** Customer and Authorized Users are responsible for protecting Account Credentials, using the Services securely, maintaining appropriate security for their systems and networks, and promptly notifying Company of any suspected unauthorized access to or use of the Services.

8. Data Retention.

- a.** We retain personal information for as long as reasonably necessary to provide, operate, support, secure, improve, and administer the Services; maintain business and accounting records; comply with legal, contractual, audit, and regulatory obligations; resolve disputes; enforce agreements; and protect rights, safety, and security.
- b.** Retention periods may vary depending on the type of information, the applicable Order Form, Customer instructions, backup and archival practices, legal requirements, and operational needs. After expiration or termination of Customer's access to the Services, Company may retain information as permitted by the Terms, this Privacy Policy, applicable law, and Company's recordkeeping practices.

9. Cookies, Analytics, and Similar Technologies.

- a.** We may use cookies and similar technologies to remember settings, authenticate users, operate and secure the Services, understand usage, improve performance, troubleshoot errors, and analyze trends.
- b.** Browser or device settings may allow users to disable certain cookies or similar technologies. Disabling technologies required for authentication, security, preferences, or core functionality may affect availability or operation of the Services.

10. Privacy Choices and Rights.

- a.** Customers and Authorized Users may update certain account information and notification preferences through settings made available within the Services or by contacting Company.
- b.** Depending on applicable law, individuals may have rights to request access to, correction of, deletion of, portability of, restriction of, or objection to certain processing of personal information, and may have the right to withdraw consent where processing is based on consent. Company may need to verify the request and may direct requests concerning Customer-controlled data to the applicable Customer.
- c.** Authorized Users should direct requests regarding Customer-controlled account information or Customer Data to the Customer account administrator unless Company is required by applicable law to respond directly.

11. Children and Age Requirements.

- a.** The Services are not intended for children or individuals under 18 years of age, or the age of majority in the Authorized User's state of residence if greater. Company does not knowingly collect personal information from children through the Services.

12. International Data Transfers.

- a.** Company is based in the United States, and information processed through the Services may be stored or processed in the United States or other locations where Company, its affiliates, or its service providers operate. By using the Services, Customer and

Authorized Users understand that information may be transferred to and processed in jurisdictions that may have data protection laws different from those in their location.

13. Third-Party Services and Links.

- a. The Services may contain links to or be used with third-party websites, services, hardware, communications networks, payment processors, or other third-party resources. Company is not responsible for the privacy, security, or data practices of third parties, and their practices are governed by their own terms and policies.

14. Changes to This Privacy Policy.

- a. Company may modify this Privacy Policy from time to time. The “Last Updated” date identifies when this Privacy Policy was last revised. Continued use of the Services after a revised Privacy Policy becomes effective constitutes acceptance of the revised Privacy Policy to the extent permitted by law.

15. Contact Us.

- a. Questions or requests regarding this Privacy Policy or Company’s privacy practices may be directed to Vigilant Aerospace Systems, Inc., Attn: Privacy, 1000 W Wilshire Blvd., Suite 224, Oklahoma City, OK 73116-7020, or through the contact method designated by Company on its website or in the applicable Order Form.