



ComposeAlpha Partner Security Policy

Last updated: July 17, 2026

This Security Policy describes the security controls, incident response practices, and vulnerability management program that Infostretch Corporation dba Apexon ("Apexon," "we," "us") applies to the ComposeAlpha application and its supporting infrastructure. This document supplements, and is separate from, our Privacy Notice, which addresses how we handle personal data. This Security Policy addresses how we protect the systems, application, and data associated with ComposeAlpha as the app vendor.

1. Security Governance

Apexon maintains an information security program aligned with recognized industry frameworks, including ISO/IEC 27001 principles. Our security program is owned by Apexon's security leadership and is reviewed on a periodic basis to reflect changes in the threat landscape, our technology stack, and applicable regulatory requirements (including GDPR and PCI DSS where relevant to specific engagements).

- A designated security team is responsible for the security of ComposeAlpha and its supporting AWS infrastructure.
- Security policies are reviewed at least annually and updated as needed.
- Employees and contractors with access to ComposeAlpha systems complete periodic security awareness training.

2. Shared Responsibility Model

Security of ComposeAlpha is a shared responsibility between Apexon and the customer/Atlassian site administrator. The table below summarizes the split at a high level.

Apexon is responsible for:

- Security of the ComposeAlpha application code, its hosting infrastructure, and the underlying AWS environment.
- Encryption, access control, vulnerability management, and incident response for systems Apexon operates.
- Secure software development practices and timely patching of the application and its dependencies.

The customer/site administrator is responsible for:

- Managing which users and groups within their Atlassian site are granted access to ComposeAlpha.
- Safeguarding their own Atlassian account credentials and enabling MFA on their Atlassian accounts.
- Reviewing and approving the OAuth scopes/permissions requested by ComposeAlpha before installation.
- Promptly revoking ComposeAlpha's access if it is no longer in use.

3. Security Incident and Breach Response



Apexon maintains a documented incident response process for identifying, containing, and remediating security incidents affecting ComposeAlpha.

3.1 Detection and Escalation

- Security events are monitored through logging and alerting on the systems supporting ComposeAlpha.
- Suspected incidents are triaged and escalated to Apexon's security response team on an urgent basis.

3.2 Containment, Eradication, and Recovery

- Confirmed incidents are contained to limit impact, followed by root-cause remediation and validation that the issue has been resolved before systems are returned to normal operation.

3.3 Notification

- Where a security incident is confirmed to have affected Customer data, Apexon will notify affected customers without undue delay and in accordance with applicable legal and contractual obligations, providing available details on the nature of the incident, data involved, and remediation steps taken.

3.4 Reporting a Security Issue

Security issues, suspected vulnerabilities, or incidents related to ComposeAlpha can be reported to Apexon at security@apexon.com. We aim to acknowledge reports within [X] business days.

4. Vulnerability Management

Apexon operates a vulnerability management program covering the ComposeAlpha application, its dependencies, and underlying cloud infrastructure.

- Regular vulnerability scanning is performed against application and infrastructure components.
- Dependency and library vulnerabilities are tracked and remediated based on severity, with critical and high-severity issues prioritized for expedited patching.
- Periodic penetration testing and/or security code review is performed on ComposeAlpha to identify and remediate security weaknesses.
- Patch management processes ensure operating systems, frameworks, and third-party components are kept up to date.
- Publicly disclosed CVEs affecting components used by ComposeAlpha are monitored via dependency/vulnerability feeds, triaged for applicability, and remediated according to severity-based timelines.
- Findings are tracked to closure through an internal remediation workflow with defined SLAs by severity.

5. General Security Controls

5.1 Access Control

- Access to ComposeAlpha production systems and Customer data is restricted on a least-privilege, role-based basis.

- Multi-factor authentication (MFA) is required for administrative access to production systems.
- Access is reviewed periodically and revoked promptly upon role change or termination.

5.2 Encryption

- Data in transit is encrypted using TLS 1.2 or higher.
- Data at rest is encrypted using AES-256 (or equivalent industry-standard encryption) via AWS-managed encryption services.
- Encryption keys are managed through a dedicated key management service rather than embedded in application code, with access to keys restricted and audited.

5.3 Network and Infrastructure Security

- ComposeAlpha is hosted on AWS infrastructure with network segmentation, security groups, and firewall controls restricting access to production environments.
- Administrative interfaces are not exposed to the public internet without additional access controls.
- Web-facing components are protected by a web application firewall (WAF) and rate limiting to mitigate common web attacks and abusive traffic; DDoS protection is provided through AWS infrastructure-level safeguards.
- Physical security of the underlying data centers is managed by AWS as part of the AWS shared responsibility model, and AWS data centers are certified against recognized standards (e.g., ISO 27001, SOC 2).

5.4 Application Security

- Secure development lifecycle (SDLC) practices are applied, including code review and security testing prior to production release.
- Credentials and secrets are managed using secure secret-management mechanisms rather than being hardcoded in application code, with periodic rotation.
- User and API sessions are subject to defined expiry and are invalidated on logout or credential revocation.

5.5 Logging and Monitoring

- System and application logs are retained to support security monitoring, investigation, and audit requirements.
- Automated alerting is configured for anomalous or suspicious activity on production systems.

5.6 Business Continuity and Data Resilience

- Data backups are performed on a regular schedule and tested periodically to confirm recoverability.
- Infrastructure is architected for resilience, with defined recovery procedures in the event of a service disruption.

5.7 Third-Party and Sub-processor Risk

- Third-party service providers and sub-processors that support ComposeAlpha are assessed for security practices prior to onboarding and are bound by confidentiality and security obligations consistent with this policy.



6. Compliance

Apexon aligns its security practices with recognized frameworks and, depending on the engagement, may be subject to standards such as ISO/IEC 27001, PCI DSS, and GDPR. Customers requiring specific compliance attestations or documentation may contact us at security@apexon.com.

7. Authentication and Access to Atlassian Data

ComposeAlpha authenticates with Atlassian using [OAuth 2.0 / JWT — confirm actual method]. Access tokens and any API credentials used by the app are stored using secure secret-management mechanisms and are never stored in plaintext or embedded in application code.

- ComposeAlpha requests only the Atlassian scopes/permissions required for its functionality, following the principle of least privilege.
- Tokens are transmitted only over encrypted (TLS) connections and are rotated or revoked in line with Atlassian's platform requirements.

8. Data Residency

Customer data processed by ComposeAlpha is hosted on Amazon Web Services (AWS) infrastructure in [region(s) — e.g., US / EU, confirm actual region(s)]. [If applicable: customers may request a specific data residency region as part of their agreement.]

9. Cross-Border Data Transfers

Where Customer data is transferred across borders (for example, between the customer's region and the region where ComposeAlpha is hosted), Apexon relies on appropriate transfer mechanisms, such as Standard Contractual Clauses (SCCs), consistent with applicable data protection law. [Confirm actual transfer mechanism and whether cross-border transfer applies to your hosting setup.]

10. Sub-processors

Apexon engages a limited number of sub-processors to support the delivery of ComposeAlpha (for example, cloud infrastructure and monitoring providers). A current list of sub-processors is available at [link, or: available upon request at security@apexon.com]. Sub-processors are contractually bound to data protection and security obligations consistent with this policy and our Privacy Notice.

11. Responsible Disclosure

Apexon welcomes reports from external security researchers who identify potential vulnerabilities in ComposeAlpha. Researchers are asked to report findings to security@apexon.com and to refrain from publicly disclosing an issue until it has been investigated and, where applicable, remediated. We do not pursue legal action against researchers who make a good-faith effort to report vulnerabilities responsibly and avoid privacy violations, data destruction, or service disruption. [Add bug bounty program details here if one exists.]

12. Data Retention and Deletion

- Customer data is retained for the duration of the customer relationship and as required to provide the ComposeAlpha service.
- Upon termination of a customer's use of ComposeAlpha, data associated with that customer is deleted or anonymized within [X days] of offboarding, except where retention is required by law or active dispute.
- Backup copies are subject to the same deletion timelines, accounting for standard backup rotation cycles.

13. Incident Severity and Response Targets

Security incidents are classified by severity, with corresponding response time targets:

- Critical (active exploitation, confirmed data exposure): investigation begins within [X hours]; customer notification per Section 3.3.
- High (significant vulnerability, no confirmed exploitation): investigation begins within [X hours/business day].
- Medium/Low (limited impact): triaged and addressed as part of regular remediation cycles.

[Confirm actual internal SLA targets before publishing — figures above are placeholders.]

14. Disaster Recovery Objectives

- Recovery Point Objective (RPO): [X hours — confirm actual figure]
- Recovery Time Objective (RTO): [X hours — confirm actual figure]

Backup and recovery procedures are tested periodically to validate that these objectives can be met in practice.

15. Change Management

- Code changes to ComposeAlpha go through peer review prior to merge.
- Changes are tested in a non-production environment before release.
- Production deployments require approval and are logged for auditability.
- Emergency changes (e.g., critical security patches) follow an expedited path but are documented and reviewed after the fact.

16. Personnel Security

- Employees and contractors with access to ComposeAlpha production systems or Customer data undergo background screening consistent with local law prior to onboarding, where permitted.
- All personnel with system access are bound by confidentiality obligations.
- Access is granted based on role and job function and is revoked promptly upon offboarding or role change.



- Security awareness training is completed at onboarding and at least annually thereafter, covering topics such as phishing/social engineering, secure handling of credentials, data classification, and incident reporting procedures. [Confirm actual training cadence and content.]

17. Customer Audit Rights

Customers may request reasonable information to verify Apexon's compliance with this Security Policy, such as a summary of the most recent penetration test findings, evidence of applicable certifications, or responses to a security questionnaire, subject to confidentiality protections. Requests can be directed to security@apexon.com. [Confirm whether formal audit rights are also addressed in the customer's contractual agreement/DPA.]

18. Cyber Liability Insurance

Apexon maintains cyber liability insurance coverage appropriate to the nature and scale of the services provided. [Confirm actual coverage details/whether this statement should be included, and whether a certificate of insurance can be made available on request.]

19. Changes to This Policy

We may update this Security Policy from time to time to reflect changes in our security practices or applicable requirements. The "Last updated" date at the top of this document reflects the most recent revision.

20. Document Revision History

- July 17, 2026 — Initial publication of standalone Partner Security Policy.

21. Contact Us

For questions about this Security Policy, or to report a security issue or incident, please contact us at security@apexon.com.