NATURALREADER SECURITY OVERVIEW

Version: 1.0
Date: July 25th, 2026

This document describes NaturalSoft's current security approach. It is intended for customers and procurement teams and does not disclose sensitive internal security details.

1. Infrastructure

- Primary production systems are hosted in an AWS region in the United States.
- Customer documents and projects may be stored in private AWS storage, including Amazon S3.
- NaturalSoft uses authorized AI, speech, authentication, analytics, payment, and support providers.
- Production access is controlled through authenticated accounts and application authorization.

2. Authentication

NaturalReader supports:

- email and password authentication through AWS Cognito;
- Google sign-in; and
- Apple sign-in.

End-user multi-factor authentication is not currently available.

Users should use strong, unique passwords and protect their email and social-login accounts.

3. Internal Access

Access to production systems and confidential customer information is limited to personnel who require it for their responsibilities.

Authorized personnel are subject to confidentiality obligations.

4. Encryption

Data in Transit

Supported NaturalReader clients communicate with NaturalReader services using HTTPS with TLS 1.2 or higher.

Data at Rest

Stored production data uses:

- AES-256 encryption; or
- equivalent cloud-provider-managed encryption.

Cloud storage is configured as private and is not intended to be publicly accessible.

5. Authorization and Customer Separation

Documents and projects are associated with authenticated users, teams, or institutions.

Access is controlled through account identity and application permissions.

Organization and EDU administrators may have access to account-management and shared-content functions.

6. Data Use

Customer Content is processed only to:

- provide the Services;
- secure the Services;
- maintain the Services;
- provide support;
- prevent abuse;
- enforce agreements; and
- comply with law.

Customer Content is not used to train NaturalSoft or third-party AI models.

7. Retention and Deletion

- Personal documents may be retained for up to two years.
- Commercial project files may be retained for up to two years.
- Operational logs are generally retained for 30 days.
- Users may delete supported documents and projects at any time.
- Account login information is deleted from active systems immediately after account deletion.
- Other active account data is deleted within 24 hours, subject to lawful and technical exceptions.
- Residual encrypted copies may remain in backups until overwritten.

8. Logging and Monitoring

NaturalSoft maintains operational, diagnostic, and security logs for:

- availability;
- troubleshooting;
- fraud prevention;
- abuse detection;
- security monitoring; and
- incident investigation.

Access to logs is restricted.

9. Development and Change Practices

NaturalSoft applies software development, testing, deployment, review, and change-management practices appropriate to the Services.

- peer code review;
- automated dependency scanning;
- vulnerability scanning;
- secrets scanning;
- penetration testing;
- release approvals;and
- security training.

10. Incident Response

NaturalSoft maintains procedures for:

- detection;
- assessment;
- containment;
- investigation;
- remediation;
- recovery;
- notification; and
- post-incident review.

Customers are notified of confirmed incidents affecting their information as required by applicable law and contract.

11. Availability and Recovery

The hosted-service availability target is 99.5%.

NaturalSoft uses cloud infrastructure, monitoring, backups, and recovery procedures appropriate to the Services.

12. Service Providers

NaturalSoft reviews providers based on relevant:

- privacy;
- security;
- reliability;
- technical;
- contractual; and
- business considerations.

Providers receive only information reasonably necessary for their function.

NaturalSoft relies in part on certifications maintained by major cloud providers. These certifications do not constitute certification of NaturalSoft.

NaturalSoft is not currently certified to SOC 2 or ISO 27001.

13. Payments

Stripe processes direct website payments.

NaturalSoft does not store full payment-card numbers.

Apple and Google process applicable mobile purchases.

14. Customer Responsibilities

Customers are responsible for:

- assigning accounts only to authorized users;
- promptly removing former users;
- protecting credentials;
- securing user devices;
- configuring sharing functions appropriately;
- avoiding unnecessary sensitive data;
- protecting downloaded files; and
- reporting suspected security incidents.

15. Security Contact

Security concerns may be reported to:

Security Email: security@naturalreaders.com

Initial reports should not contain passwords, full payment-card information, or unnecessary sensitive Customer Content.