NeoShield

Security Review Package

Last reviewed: 2026-10-30

This package reproduces the statements published on the NeoShield Trust Center. It is not a certification, an audit report or a penetration-test report. Items marked as a self-assessment were produced by automated checks run by NeoShield itself.

No commissioned third-party penetration-test report is currently published.

Company and service information

Service

NeoShield: passive website security reporting and fix verification for freelance web developers and small web agencies, plus a secondary library of free security tools.

Operator details

Seller, address and contact details required under Japan's Specified Commercial Transactions Act are published on the legal disclosure page.

Where it is run

NeoShield is operated from Japan. Operations rely on automation and written procedures (see Operational continuity).

Service overview document

Contact us for security documentation.

Security of NeoShield at a glance

TLS encryption

Every page and API is served over HTTPS, with a Strict-Transport-Security header (one year) so returning browsers use HTTPS only.

Passwordless sign-in

A single-use code sent by email, valid for 5 minutes, stored only as a keyed hash and rate limited. There are no passwords to leak. It is one factor, not multi-factor authentication.

Stripe-hosted checkout

Card details are entered only on Stripe's pages and never reach NeoShield. A plan is granted only after the payment is confirmed with Stripe (signed webhook or a server-side check of the checkout session).

Data retention

Security logs are deleted after 30 days, only the 100 most recent reports per account are kept, and account deletion is completed within 30 days. See Data retention below.

Vulnerability disclosure

A public disclosure policy with safe-harbor terms and a security.txt contact. No paid bug bounty.

Dependency maintenance

No third-party PHP packages or frameworks. One small vendored JavaScript library (QR codes) is pinned by hash and listed in a CycloneDX software bill of materials. The PHP version is set by the operator in the hosting panel; when a PHP security advisory affects the service, request-level mitigations are added until the patched version is applied (release 2.21.1 is an example).

Logging

Security events such as sign-ins, rate limiting, denied access, scans, payments and plan changes are recorded with time, event type, IP address, browser identifier and account email. Sign-in codes, passwords, card numbers and API keys are not written to logs. Logs are deleted after 30 days and can be read only from administrator accounts, which today means the operator.

Certifications

No SOC 2 report and no ISO/IEC 27001 certification. Nothing on this page should be read as implying either.

Security practices

Application security

Prepared statements, CSRF tokens on state-changing forms, SSRF guards on outbound requests, and security headers. The Content-Security-Policy limits scripts to this site for visitors who have not consented to analytics or advertising; with that consent, Google origins and inline scripts are allowed. Inline styles are allowed for everyone.

Change integrity

File-integrity monitoring over the codebase with an HMAC-protected SHA-256 baseline, and a daily job that re-verifies controls and alerts on regressions.

Testing

Internal testing with the platform’s own scanning and audit tooling on each release, and an automated test suite.

Scanner behaviour

The website scanner sends a limited number of ordinary requests to publicly accessible pages and reads DNS records. It does not exploit, brute-force, fuzz or log in. Only ports 80 and 443 are used; internal, private, link-local, metadata and reserved addresses are blocked, including after redirects and DNS resolution. Scheduled monitoring requires proof of domain control (DNS TXT record or a file on the site), re-checked weekly.

Data processing

What is stored

Your e-mail address as the account identifier, plus operational records: sign-in times and role, plans and purchases, Academy progress, messages you send, security events (IP address and truncated browser identifier), scan targets and reports, and workspace data such as SOC events, assets and incidents. The full list is in the Privacy Policy.

Scan data

A scan report contains the target host, its resolved IP address, observed response headers and findings. Reports are stored against your account only.

Never stored

Card numbers (payments run on Stripe’s hosted checkout) and passwords (sign-in uses single-use email codes stored only as keyed hashes).

Analytics

Product analytics receive event names and coarse categories only. Scanned URLs, findings, evidence, emails and payment details are never sent to analytics providers.

Data retention

Security and activity logs

Removed automatically after 30 days.

Scan reports

The most recent 100 reports per account are kept. Paid accounts can delete any report at any time.

Payment records

Kept for accounting; fulfilled checkout references are kept for 45 days to prevent double grants.

Details

See How long we keep it in the Privacy Policy.

Data location

Hosting

The application is hosted by Hostinger. The hosting region is available on request.

International transfers

Anthropic, Stripe and Google may process relevant data in the United States and other countries, as described in the Privacy Policy.

Encryption

In transit

HTTPS for every page and API.

At rest

Secrets we issue (sign-in codes, verification tokens, agent and API keys, team-invite tokens) are stored only as hashes. Scan reports, finding records and account records are not encrypted at the application level; they rely on the hosting provider's storage protections. Quantum Vault encrypts text in server memory and stores nothing.

Authentication and account protection

Sign-in

Passwordless sign-in with a single-use e-mail code that expires after 5 minutes and is stored only as a keyed hash. This is one factor, not multi-factor authentication.

Sessions

HttpOnly, Secure, SameSite=Lax session cookie with an idle timeout of 30 minutes. Lax is used so the session survives the return from Stripe checkout; every state-changing form is also CSRF-token protected.

Abuse protection

Sign-in code requests and code entry are rate limited per e-mail address, per IP address, per network (/24 or /48) and per account; metered actions are rate limited per account; website scans also have per-organization and global concurrency limits.

Session control

Sessions end after the idle timeout or 12 hours after sign-in. The account page lists signed-in sessions and can sign out any of them or all others, enforced on the server.

Multi-factor authentication and SSO

Not available yet. Passkeys (WebAuthn) for administrators, workspace owners and sensitive actions are planned; until then, exporting or deleting account data requires a sign-in within the last 15 minutes.

Subprocessors

Hostinger

Purpose: Application hosting, database and file storage
Data categories: All service data: account, plan, payment reconciliation, scan reports, findings, client lists, logs
Location: Hosting region available on request
Receives scan content: Yes (stores it)
Model training: Not applicable
Retention: As set by NeoShield (see Data retention)
`https://www.hostinger.com/legal/privacy-policy`

Stripe

Purpose: Payment processing on Stripe-hosted checkout
Data categories: Email, payment details entered on Stripe, amount, plan code
Location: United States and other countries
Receives scan content: No
Model training: Not applicable
Retention: Per Stripe's policy
`https://stripe.com/privacy`

Anthropic

Purpose: Optional AI-assisted prioritization in the scanner and other AI features
Data categories: Target hostname, scores and finding text for the scan; never your email or IP address
Location: United States
Receives scan content: Yes: for manual scans only when AI-assisted prioritization is switched on; scheduled monitoring scans currently always include it
Model training: Governed by Anthropic's commercial terms (see provider link)
Retention: Per Anthropic's commercial terms

https://www.anthropic.com/legal/privacy

Google

Purpose: Analytics and advertising, each only after your consent; advertising only on blog articles and never while signed in
Data categories: Event names and coarse categories; standard advertising cookies where shown
Location: United States and other countries
Receives scan content: No
Model training: Per Google's policy
Retention: Per Google's policy
https://policies.google.com/privacy

PostHog

Purpose: Product analytics, only if enabled by the operator
Data categories: The same event names and coarse categories as above
Location: As configured by the operator
Receives scan content: No
Model training: Per PostHog's policy
Retention: Per PostHog's policy
https://posthog.com/privacy

AI processing

Model output

Treated as untrusted data. No AI-authored code is executed on NeoShield servers.

Accuracy

AI output can be wrong or incomplete. Findings show their evidence so you can review them before acting.

Optional

AI-assisted prioritization can be switched off for each manual scan. Scheduled monitoring scans currently always include it.

Data deletion

Scan reports

Paid accounts can delete individual reports from scan history.

Account data

Download your data and request account deletion from the account page. Deletion is confirmed by e-mail and completed within 30 days; purchase records are kept as required by law and backups rotate out on their schedule. Correction and other requests: security@neoshieldsecurity.com.

Incident response

Procedure

A documented incident-response and continuity runbook covers triage, containment, recovery and customer communication.

Customer notification

Affected customers are contacted by email. A formal notification SLA is not currently published.

Vulnerability disclosure

Policy

Good-faith research is welcome under the Responsible Disclosure policy, which includes safe-harbor terms.

security.txt

Published at /.well-known/security.txt (RFC 9116).

Bug bounty

No paid bug bounty programme is currently offered.

Operational continuity

Backups

Automated backups of account, plan, payment, scan-report, finding and client records, run by the daily maintenance job with the newest 14 kept. Backups are stored on the same hosting account in a web-denied directory; off-site copies are not currently made automatically.

Failover

If the database is unavailable, the application falls back to file-based storage so sign-in and scanning keep working. This is a degraded mode, not a replicated database.

Recovery objectives

Internal targets (not contractual): recovery point within 24 hours and recovery time within 2 business days for the core service.

Restore testing

A restore procedure is written in the operations runbook. A completed restore test has not yet been evidenced, so treat the recovery targets as goals.

Monitoring and alerting

A daily self-check backs up data, verifies file integrity, re-runs the internal control self-assessment and emails the operator when anything regresses. Failed scheduled scans and failed payment or email deliveries are recorded on the status page.

Incident communication

Affected customers are contacted by email, and the status page shows the incident. There is no published notification deadline.

Outside support hours

Scans, scheduled monitoring, sign-in and payments run automatically. Support replies, refunds and manual fixes wait until support resumes. There is no on-call rota.

Support limits

Email and the contact form only, no live chat or phone. Free: best effort. Pro: aimed within 2 business days. MSP / Team: answered before Free and Pro, with no guaranteed response time.

Service status

Status page

The status page is generated automatically from recorded outcomes of sign-in e-mail, AI calls, scans, scheduled jobs, payments and threat-intelligence refresh, and shows the time of the last check and an incident history.

Uptime commitment

No uptime guarantee or SLA is currently offered.

Certifications and independent assessments

ISO/IEC 27001

Not currently certified.

SOC 2

No SOC 2 report. Independent assessment not currently published.

PCI DSS

Not applicable to NeoShield’s own systems: card data is entered only on Stripe’s hosted checkout.

Independent penetration test

No commissioned third-party penetration-test report is currently published.

Automated self-assessment

Automated technical control checks run against the live system; the evidence report is clearly labelled a self-assessment and is available on request.

Cyber insurance

Information available on request.

Latest self-assessment

32 of 36 automated controls passing, assessed July 21, 2026. This is a self-assessment, not an audit.

Security contact information

Security and privacy

security@neoshieldsecurity.com

General enquiries

Contact form

Vulnerability reports

See the Responsible Disclosure policy.

Questions about this package: security@neoshieldsecurity.com