

Security and Data Protection Overview

Last updated: 2026-07-30

1. Status and scope

This page gives a high-level, public description of safeguards applied to the `inai.world` company website. It is informational, is not a certification or audit report, and does not create a service level, warranty or response-time commitment.

Product-specific security, processing and deployment obligations exist only where stated in the applicable product terms, data-processing terms, order form or signed agreement.

This public page deliberately does not disclose INAI's private application, email, domain, supplier or infrastructure inventory.

2. Public website safeguards

The current Website implementation includes:

- HTTPS delivery through the Website host;
- response headers intended to reduce content-type confusion, framing and unnecessary browser permissions;
- an enforced Content Security Policy and HTTP Strict Transport Security;
- public-form request sizes enforced against the actual streamed body;
- validation of required form fields and email format;
- distributed contact-form rate limiting based on limited request information;
- a hidden anti-spam field on the main contact form; and
- file-type and size restrictions on the pilot upload form.

These controls reduce common risks but cannot eliminate every risk associated with internet services.

3. Data minimisation and access

Public forms request information according to the selected contact route. Visitors should provide only information needed for their enquiry and should not submit credentials, payment data, unnecessary sensitive data or confidential third-party material.

Form submissions are routed to the relevant inAi team role address. Access should remain limited to people handling the relevant request and technical services needed to deliver or protect it.

Details of the data collected, purposes, recipient categories, retention criteria and rights are in the [Global Privacy Policy](#).

4. Browser storage and tracking

The Website currently stores only the first-party light or dark theme preference described in the [Cookie and Local Storage Policy](#).

The Website does not currently deploy advertising, cross-site tracking or audience-measurement cookies.

5. Security reports

Potential security issues concerning the Website may be reported to the inAi team at security@inai.world.

A useful report should include, where safe:

- the affected page or function;
- steps needed to reproduce the issue;
- the observed and expected behaviour;
- the potential impact; and
- any non-sensitive supporting material.

Do not include credentials, private keys, access tokens, personal data belonging to others or destructive proof.

INAI does not publish an acknowledgement, assessment, remediation or update timeline and does not promise a bounty or public credit. Any legally required incident or personal-data notification is handled under the applicable law and agreement.

6. Privacy and other enquiries

- Security reports: security@inai.world
- Privacy questions and rights requests: privacy@inai.world
- General enquiries: contact@inai.world

These addresses are role addresses received by the inAi team. No individual security or privacy recipient is designated by this page.