security.en

Security and Data Protection Statement

Service: AINet (https://ainet.bytestrike.dev)

Version: 2026-05-13.

Security contact: security@bytestrike.dev

---

1. Purpose

This document describes AINet’s public security principles. It is not a technical runbook, infrastructure diagram, or list of internal protection mechanisms. Implementation details that could help attack the Service are intentionally not disclosed.

2. Principles

2.1. **Data minimization.** The Service collects and stores only data needed for accounts, API access, billing, abuse prevention, security, and support.

2.2. **Content statelessness.** AINet does not store model request texts or model response texts on its side.

2.3. **Secret separation.** User API keys, session tokens, 2FA data, and upstream provider keys are treated as secrets and are not stored in plaintext.

2.4. **Risky feature limits.** The Service restricts features that may create provider-side file storage, conversation state, or bypass the stateless model.

2.5. **Legal and risk restrictions.** Access for specific user categories or use cases may be restricted at network and application levels. Such restrictions are based on technical network signals and risk policy and are not passport, citizenship, or tax residence verification.

3. Transfer and Storage

3.1. Data is transmitted between the user, Service infrastructure, and upstream providers through protected communication channels.

3.2. Request content is transmitted to Anthropic or OpenAI to perform the request. The Operator does not have a Zero Data Retention agreement with those providers, so their own retention policies remain applicable.

3.3. AINet does not store:

- prompt, message, or instruction texts;
- model response texts;
- raw user API keys;
- plaintext upstream provider keys;
- bank card or bank account data.

3.4. Technical and billing metadata may be stored to operate the Service: account and request identifiers, selected provider/model, processing status, usage counters, credit/debit amounts, payment identifiers, and audit records.

4. Accounts and Access

4.1. API access uses API keys. Users are responsible for storing keys in a protected environment and must revoke a key immediately if compromise is suspected.

4.2. The Service applies usage limits and anti-abuse controls to protect users, balances, and infrastructure.

4.3. Administrative actions are restricted to privileged access and are audited. Audit records are not intended to store user prompts or outputs.

5. Payments

5.1. The Service accepts cryptocurrency payments through connected payment providers. AINet stores technical payment identifiers and balance records needed for crediting, debiting, refunds, and dispute resolution.

5.2. AINet does not process or store bank card, bank account, or fiat payment details.

6. Limitations and Fair Disclosure

6.1. No system can guarantee absolute security. AINet applies reasonable technical and organizational measures, but incident risk cannot be fully eliminated.

6.2. AINet does not control the internal security, availability, or retention policies of Anthropic, OpenAI, Cloudflare, hosting providers, or payment providers.

6.3. Users should not send third-party personal data, passwords, tokens, private keys, seed phrases, trade secrets, NDA materials, banking data, or other sensitive information in prompts without a legal basis and understanding of upstream transfer risks.

7. Vulnerabilities

If you discover a vulnerability, report it to security@bytestrike.dev before public disclosure.

Good-faith research must not include:

- access to other accounts, data, keys, or sessions;
- API key guessing or credential stuffing;
- DoS/DDoS or load testing without permission;
- bypassing billing, limits, or access restrictions;
- publication of exploit details before remediation.

8. Related Documents

- Terms of Service - `/legal/terms.en.md`
- Privacy Policy - `/legal/privacy.en.md`
- Acceptable Use Policy - `/legal/aup.en.md`

Version dated 2026-05-13.