Velithon

Trust & Service Status Statement

Table of Contents

Last updated: 13 May 2025 • Contact: security@velithon.com

Trust & Service Status Statement

1. Our Commitment to Transparency

Velithon believes that openness regarding reliability and security fosters user trust. This Statement outlines our high-level practices and the status of the prototype environment. Because the platform is evolving quickly, details will mature over time; however, the principles below guide our operations from day one.

2. Uptime Philosophy

While the prototype is pre-commercial, we still monitor core endpoints around the clock. Outages or significant degradations, should they occur, will be acknowledged publicly on a dedicated status page reachable from the site footer. Historical uptime percentages may be published as the service stabilises but are not contractually binding.

3. Incident Handling

We classify incidents by severity and follow a simple cycle: detection, analysis, mitigation, retrospective. If an event affects user confidentiality, integrity or availability in a material way, we will issue a concise incident note on the status page, including root cause and remediation steps when known.

4. Security by Design

Security controls include:

- encrypted connections (TLS) for all external traffic;
- one-way hashing of passwords and key material;
- principle-of-least-privilege access and periodic credential rotation;
- separation of development and production data;
- static and dynamic code analysis during development.

5. Privacy and Data Protection

Our Privacy Policy describes how we handle personal data. In brief: only the minimum data required to run a wait-list and prototype accounts is collected; raw blockchain and social-media identifiers are processed for analytics without attempting to link them to real-world individuals. Any future processor or sub-processor will be vetted for security and privacy compliance before personal data is shared.

6. Responsible Disclosure Program

We welcome good-faith reports of potential vulnerabilities. Security researchers may write to security@velithon.com using plain text or an encrypted attachment. We aim to acknowledge receipt within two business days and keep you informed as we triage and remediate. We ask researchers to give us a reasonable opportunity to fix issues before any public disclosure.

7. Planned Enhancements

The following initiatives are on our roadmap and will be reflected in later versions of this Statement:

- optional multi-factor authentication for all user types;
- region-specific data residency choices;
- external third-party penetration testing;
- broader uptime metrics once the service leaves prototype stage;
- transparency reports summarising government data-access requests (if any).

8. Versioning

When we materially expand or clarify practices, we will publish a new version with a revised “Last updated” date and, where feasible, notify registered participants. Older versions remain archived for reference.