

Terms and Conditions

Service: Origin Secured Event Chain & Trust Orchestration Infrastructure

Service Type: Infrastructure Software as a Service (iSaaS)

1. Agreement Structure and Priority

1.1 This Agreement comprises:

- a) these Terms and Conditions (the “Terms”);
- b) the Order Form / Statement of Work (SOW) (including service configuration, pricing, term, and any agreed implementation services);
- c) the Service Definition (service description, scope, intended users, security, availability, support, onboarding/offboarding);
- d) the Pricing Document;
- e) the Data Processing Agreement (DPA) referenced at clause 6; and
- f) Documentation (including API documentation and operating environment requirements).

1.2 **Order of precedence** in the event of conflict:

- a) Order Form / SOW;
- b) these Terms;
- c) Service Definition;
- d) Pricing Document;
- e) DPA;
- f) Documentation.

1.3 Customer terms and conditions are excluded unless expressly agreed in writing and signed by both parties.

2. Definitions

Key terms used in these Terms include:

- **“Customer”**: the contracting public sector buyer and/or its delivery partners as stated in the Order Form/SOW.
- **“Authorised Users”**: Customer staff/contractors approved to administer or integrate with the Service (including gateway admins), within any limits set out in the Order Form/SOW.
- **“Digital Licence”**: a cryptographically signed trust artefact representing an entity (e.g., person/community/AI/asset/business), issued and lifecycle-managed in the Service.
- **“Event Chain Digital Licence”**: the licensed capability enabling immutable, append-only trust event recording and provenance.
- **“Orchestration Digital Licence”**: the licensed capability enabling orchestration, governance, policy enforcement and challenge/verification flows.

- **“Customer Data”**: data input/uploaded/provided by Customer or Authorised Users (including personal data) for the purpose of using the Service.
 - **“Documentation”**: user guides, admin guides, API documentation, operating environment requirements, and other materials made available by Origin Secured.
 - **“DPA”**: Origin Secured’s Data Processing Agreement at: <https://originsecured.com/data-processing-agreement>
 - **“Service”**: Origin Secured Event Chain & Trust Orchestration Infrastructure, including secure APIs, admin gateways, tenant configuration, artefact management, verification and revocation.
 - **“Third Party Materials”**: third-party components subject to separate licence terms.
-

3. Service Provision and Licence Grant

3.1 Subject to payment of Charges and compliance with these Terms, Origin Secured grants the Customer a **non-exclusive, non-transferable** right for Authorised Users to access and use the Service and Documentation during the Term for Customer’s internal business purposes and delivery of public services.

3.2 Where APIs are provided, Customer may use them solely to integrate Customer systems with the Service, in accordance with Documentation.

3.3 **No end-user business application licence is granted.** The Service is intended to be integrated into existing services via secure APIs and administrative gateways (as per the Service Definition).

4. Service Scope

4.1 Included and excluded scope is as described in the Service Definition.

4.2 The Service **does not** include primary identity proofing/KYC, issuance of government identity documents, buyer-specific line-of-business applications, or on-premise deployment unless expressly agreed in an Order Form/SOW.

5. Charges, Invoicing and Payment

5.1 Charges are as set out in the Pricing Document and confirmed in the Order Form/SOW, excluding VAT.

5.2 Pricing model includes:

a) **Core Administrative Infrastructure Licences**

b) **Licence State Lookup Pricing**

5.3 Unless otherwise agreed in the Order Form/SOW:

- annual fees are invoiced **annually in advance**;
- payment terms are **30 days** from invoice date.

5.4 If Customer increases Digital Licence volumes or other chargeable units, charges apply from the effective date agreed in writing. The Customer may decrease Digital License volumes annually.

5.5 Origin Secured may suspend the Service for undisputed overdue invoices where legally permissible and after giving reasonable notice.

6. Data Protection

6.1 Each party will comply with applicable Data Protection Legislation (including UK GDPR).

6.2 The parties agree that, for personal data processed by Origin Secured on Customer's behalf, **Customer is Controller** and **Origin Secured is Processor**, unless otherwise stated in the Order Form/SOW.

6.3 The DPA is incorporated by reference and available at:
<https://originsecured.com/data-processing-agreement>

6.4 Customer warrants it has a lawful basis to provide Customer Data to Origin Secured and to instruct processing.

7. Security

7.1 Security controls are as described in the Service Definition and include (as applicable):

- encryption in transit and at rest;
- strong authentication and RBAC;
- cryptographic signing of artefacts and events;
- immutable append-only event records;
- centralised logging/monitoring/alerting.

7.2 Customer is responsible for:

- securing user credentials, devices, and access paths;
- ensuring integrations and calling systems meet security requirements; and
- applying its own security governance appropriate to its use case.

8. Availability, Maintenance and Resilience

8.1 **Availability Target:** 99.9% per calendar month for production instances, as set out in the Service Definition.

8.2 Service window is 24x7x365. Planned maintenance will normally be performed outside UK business hours where reasonably possible.

8.3 The availability definition, measurement and calculation follow the Service Definition.

8.4 Origin Secured will operate redundancy, backups, monitoring, and documented recovery procedures as described in the Service Definition.

9. Support

9.1 Support channels, hours, severity levels, response targets and update cadences are as set out in the Service Definition, unless varied in the Order Form/SOW.

9.2 Exclusions apply as per Service Definition (e.g., bespoke development, buyer environment issues unrelated to the Service).

10. Customer Obligations and Acceptable Use

10.1 Customer shall:

- a) comply with these Terms and Documentation;
- b) ensure Authorised Users comply with these Terms;
- c) maintain required connectivity and operating environment;
- d) provide reasonable cooperation for support and incident investigation.

10.2 Customer shall not (and shall ensure Authorised Users do not):

- a) attempt to bypass security controls;
- b) reverse engineer, decompile, disassemble or create derivative works of the Service except to the extent permitted by law;
- c) introduce malware, attempt unauthorised access, or disrupt the Service;
- d) use the Service to create a competing product or service;
- e) misuse APIs (including credential/key sharing or abusive calling patterns).

10.3 Customer is responsible for the content, legality, integrity and accuracy of Customer Data and any instructions it provides.

11. Intellectual Property

11.1 Origin Secured and/or its licensors own all intellectual property rights in the Service, Documentation, APIs, and related materials ("OS IPR").

11.2 Customer retains all rights in Customer Data.

11.3 Customer grants Origin Secured a non-exclusive licence to process Customer Data solely to provide the Service, support, security, compliance, and to perform obligations under these Terms.

11.4 Origin Secured may use feedback to improve the Service without restriction.

12. Confidentiality

12.1 Each party will keep the other's Confidential Information confidential and use it only to perform obligations under this Agreement.

12.2 Disclosure is permitted to personnel/contractors/advisers on a need-to-know basis under equivalent confidentiality obligations, and as required by law/regulator/court.

12.3 Service details, Documentation, and performance/security testing results relating to the Service constitute Origin Secured Confidential Information.

13. Third Party Materials

13.1 Third-party components may apply. Customer agrees to comply with applicable third-party licence terms notified by Origin Secured or referenced in Documentation.

14. Liability

14.1 Nothing limits or excludes liability for: death/personal injury caused by negligence, fraud/fraudulent misrepresentation, or any liability that cannot be limited by law.

14.2 Subject to clause 14.1, neither party is liable for indirect or consequential losses, including loss of profits, revenue, anticipated savings, goodwill, or business opportunity.

14.3 Subject to clauses 14.1 and 14.2, **each party's total aggregate liability** arising in a Contract Year shall not exceed the **total Charges paid or payable** by the Customer for that Contract Year, unless a different cap is agreed in the Order Form/SOW.

14.4 Customer acknowledges the Service supports evidence and trust workflows but does not itself perform primary identity proofing/KYC, and Customer remains responsible for its operational and regulatory use of outputs.

15. Term and Termination

15.1 The Agreement term is as stated in the Order Form/SOW (default **12 months**), renewing annually unless terminated.

15.2 Either party may terminate for material breach not remedied within 30 days of written notice (or sooner where breach is not remediable).

15.3 Either party may terminate immediately for insolvency-type events affecting the other party.

15.4 Termination for convenience may be included only if stated in the Order Form/SOW (public sector buyers often require this).

16. Offboarding, Data Export and Deletion

16.1 Offboarding services are as described in the Service Definition, including export in agreed formats and secure deletion.

16.2 On termination/expiry, Origin Secured will make Customer Data available for export for a limited period specified in the Order Form/SOW (default 30 days), after which Origin Secured will securely delete Customer Data except where retention is required by law.

17. Force Majeure

Neither party is liable for failure/delay caused by events beyond reasonable control. If force majeure continues for more than 60 days, either party may terminate on written notice.

18. General

18.1 **Variation:** must be in writing and signed by authorised representatives.

18.2 **Assignment:** Customer may not assign without Origin Secured's written consent (not unreasonably withheld).

18.3 **No partnership/agency.**

18.4 **Third party rights:** none under the Contracts (Rights of Third Parties) Act 1999.

18.5 **Notices:** by email and/or post as specified in the Order Form/SOW.

18.6 **Governing law:** England & Wales; exclusive jurisdiction of courts of England & Wales.

Schedule A — Service Levels and Support (Production)

Incorporated by reference to the Service Definition, including:

- 99.9% monthly availability target for production instances
 - Support channels and hours
 - Severity levels and response/update targets
 - Maintenance approach and exclusions
-

Schedule B — Pricing (Production)

Incorporated by reference to the Pricing Document, including:

- Event Chain Digital Licence: £25,000 (one-off)
- Orchestration Digital Licence: £25,000 (one-off)
- Digital Licence (People/Community/AI/Asset): £5 per year
- Digital Licence (Business): £100 per year
(All exclusive of VAT)