

END CUSTOMER SUBSCRIPTION AGREEMENT

(TRAEMS)

<https://traems.com/>

Public sector workforce management platform (workforce scheduling, rostering, workforce operations, reporting).

This Agreement is entered into between:

- 1) Ceucure Intelligence Limited ("CIL", "Supplier", "we", "us"), a company incorporated in England and Wales (Company No. [●]) with registered office at [●]; and
- 2) [Customer legal name] ("Customer", "you"), a company incorporated in [●] (Company No. [●]) with registered office at [●].

Together, the “Parties” and each a “Party”.

KEY COMMERCIAL TERMS (SUMMARY)

Term	Value
Effective Date	[●] (as per Order Form)
Initial Subscription Term	[e.g., 12 months]
Renewal	As stated in the Order Form (default: auto-renew for successive 12-month terms unless either Party gives 30 days’ notice before renewal).
Fees	As stated in the Order Form (exclusive of VAT).
Payment Terms	14 days from invoice date unless otherwise stated in the Order Form.
Support Hours	09:00–17:00 UK business days (Standard Support) unless otherwise stated.
Monthly Uptime Target	99.9% (excluding permitted downtime).
Liability Cap (CIL)	Fees paid or payable for the Services in the preceding 12-month period (subject to mandatory legal carve-outs).
Data Protection	UK GDPR / GDPR Data Processing Addendum included (Schedule 5).

Cecure Intelligence Limited (CIL) – TRAEMS End Customer Agreement

Governing Law / Courts	England and Wales / exclusive jurisdiction.
------------------------	---

Note: This summary is for convenience. The Agreement and Schedules prevail in case of conflict.



TABLE OF CONTENTS

To update the Table of Contents in Word: Right-click → Update Field → Update entire table.



Main Terms

These Main Terms apply to the Services. Product-specific terms are in Schedule 6.

1. Definitions and interpretation

In this Agreement, capitalised terms have the meanings given in this Section and in the Schedules. In the event of conflict, the order of precedence in Section 2.3 applies.

“Order Form” means an order form, statement of work, or online order that references this Agreement and sets out the Subscription(s), Fees, and any special terms.

“Services” means the hosted software service(s), Documentation, and support described in the Order Form and the relevant Product Schedule.

“Documentation” means user guides and technical documentation made available by CIL for the Services.

“Subscription Term” means the initial term and any renewal term stated in the Order Form.

“Customer Data” means all data submitted, uploaded, or processed by or on behalf of Customer through the Services.

“Authorised Users” means individuals authorised by Customer to use the Services subject to this Agreement.

“Workforce Data” means employee/user data, scheduling, time/attendance records, operational notes, and related workforce operational information processed by the Service.

2. Agreement structure, order of precedence, and formation

2.1 Agreement components. This Agreement comprises: (a) these terms; and (b) the Schedules (including the Product Schedule, Service Levels, Acceptable Use Policy, Security Schedule, and Data Processing Addendum).

2.2 Formation. This Agreement becomes legally binding when (a) both Parties sign an Order Form; or (b) Customer clicks “I agree” (or equivalent) to accept these terms in an online ordering flow that references this Agreement.

2.3 Order of precedence. If there is a conflict: (1) the Order Form; (2) the Product Schedule; (3) the Data Processing Addendum; (4) the Security Schedule; (5) the Service Levels; (6) the Acceptable Use Policy; (7) these main terms; unless expressly stated otherwise.

3. Subscription grant and use rights

3.1 Subscription. Subject to payment of Fees and compliance with this Agreement, CIL grants Customer a non-exclusive, non-transferable (except as permitted by Section 19) right for Authorised Users to access and use the Services during the Subscription Term.

3.2 Scope. Use is limited to Customer's internal business purposes and as otherwise permitted in the Product Schedule and Order Form.

3.3 Usage limits. Subscriptions may be subject to user counts, feature tiers, storage limits, API limits, or other usage parameters stated in the Order Form. CIL may enforce limits and may charge overage Fees if specified in the Order Form.

3.4 Restrictions. Customer must not (and must not permit others to): (a) copy, modify, or create derivative works of the Services except as allowed by law; (b) reverse engineer, decompile, or attempt to extract source code except as permitted by law; (c) access the Services to build a competing product; (d) circumvent usage limits; or (e) use the Services in breach of the Acceptable Use Policy or applicable law.

3.5 Third-party services. The Services may interoperate with third-party services. Customer's use of third-party services is governed by the third party's terms. CIL is not responsible for third-party services except as expressly stated in the Product Schedule.

4. Customer responsibilities

4.1 Customer is responsible for: (a) the lawfulness, quality, and accuracy of Customer Data; (b) obtaining all necessary consents and notices to permit processing of Customer Data (including for recordings, AI features, and communications); (c) managing Authorised User access, including secure credentials; and (d) ensuring its systems and networks meet any minimum requirements notified by CIL.

4.2 Customer must promptly notify CIL of any unauthorised access and cooperate in remediation.

4.3 Customer is responsible for the acts and omissions of Authorised Users as if they were Customer's own.

5. Professional Services (if any)

5.1 Professional Services. Implementation, configuration, migration, training, and consultancy services (if any) will be described in an Order Form or statement of work. Unless otherwise stated, Professional Services are provided on a time-and-materials basis.

5.2 Assumptions. Delivery timelines depend on Customer providing timely access, approvals, and required information.

6. Security and data protection

6.1 Security. CIL will implement and maintain the technical and organisational measures set out in the Security Schedule.

6.2 Data protection. Where CIL processes personal data on behalf of Customer, the Data Processing Addendum applies and is incorporated by reference.

6.3 Security incidents. CIL will notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Data as set out in the Data Processing Addendum.

7. Support, Service Levels, and maintenance

7.1 Support. CIL will provide support in accordance with the Service Levels Schedule.

7.2 Maintenance. CIL may perform planned maintenance. Where reasonably practicable, CIL will provide advance notice and schedule maintenance to minimise disruption.

7.3 Changes. CIL may modify the Services (including features) provided it does not materially reduce core functionality during the Subscription Term (except for security, legal compliance, or deprecation of third-party dependencies).

7.4 Beta features. Beta/preview features (if any) are provided “as is” and may be changed or withdrawn. Beta features are excluded from Service Levels unless stated otherwise.

8. Fees, invoicing, and payment

8.1 Fees. Customer will pay the Fees specified in the Order Form.

8.2 Invoicing. Unless otherwise stated, Fees are invoiced annually in advance. Usage-based charges (if any) are invoiced monthly in arrears.

8.3 Payment terms. Payment is due within 14 days of invoice date unless otherwise stated in the Order Form.

8.4 Taxes. Fees are exclusive of VAT/GST and other applicable taxes, which will be added where required by law.

8.5 Late payment. Overdue amounts may accrue interest at 4% per annum above the Bank of England base rate, calculated daily.

8.6 Disputed invoices. Customer must notify CIL of any invoice dispute in writing within 15 days of invoice date, stating reasons and the undisputed portion (if any). Customer must pay undisputed amounts on time.

8.7 Fee changes on renewal. Fees may be increased on renewal by providing Customer at least 60 days' prior written notice, unless the Order Form states fixed pricing.

9. Intellectual property

9.1 CIL IP. CIL and its licensors retain all right, title, and interest in and to the Services, Documentation, and any improvements, including all intellectual property rights.

9.2 Customer Data. Customer retains all right, title, and interest in and to Customer Data.

9.3 Feedback. Customer grants CIL a worldwide, perpetual, irrevocable, royalty-free licence to use and incorporate feedback or suggestions without restriction.

9.4 Usage analytics. CIL may collect and use aggregated and de-identified usage analytics for service improvement, security, and business operations, provided it does not identify Customer or individuals.

10. Confidentiality

10.1 Each Party may receive Confidential Information from the other. The receiving Party must protect it using at least the same degree of care it uses to protect its own confidential information (and no less than reasonable care) and use it only to perform this Agreement.

10.2 Confidential Information does not include information that is (a) public through no fault of the receiving Party; (b) independently developed; (c) lawfully received from a third party; or (d) required to be disclosed by law or court order (subject to notice where permitted).

11. Warranties and disclaimers

11.1 CIL warrants that it will provide the Services with reasonable skill and care.

11.2 Except as expressly stated, the Services are provided “as is” and CIL disclaims all other warranties to the maximum extent permitted by law, including implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

11.3 Customer warrants that it has all rights necessary to provide Customer Data and to permit processing under this Agreement.

12. Indemnities

12.1 IP indemnity. CIL will indemnify Customer against losses arising from a third-party claim that the Services infringe UK intellectual property rights, provided Customer (a) promptly notifies CIL; (b) allows CIL to control the defence and settlement; and (c) provides reasonable assistance.

12.2 Exclusions. CIL has no obligation to the extent a claim arises from Customer Data, Customer modifications, use in combination with non-CIL products where the claim would not arise otherwise, or use not in accordance with Documentation.

12.3 Remedies. If infringement is likely, CIL may: procure the right to continue, modify to be non-infringing, or terminate affected Services and refund prepaid unused Fees for the affected portion.

12.4 Customer indemnity. Customer will indemnify CIL against losses arising from (a) Customer Data; (b) Customer's breach of the Acceptable Use Policy; or (c) unlawful use by Authorised Users.

13. Limitation of liability

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

13.2 Subject to Section 13.1, neither Party is liable for loss of profit, revenue, business, goodwill, or indirect or consequential losses.

13.3 Subject to Section 13.1, CIL's total aggregate liability arising out of or in connection with this Agreement in any 12-month period is limited to the Fees paid or payable by Customer to CIL for the Services in that 12-month period.

13.4 Customer's total aggregate liability in any 12-month period is limited to the Fees paid or payable by Customer in that 12-month period, except for Customer's payment obligations, breach of confidentiality, and Customer's indemnities, which are uncapped unless otherwise stated in the Order Form.

14. Suspension

CIL may suspend access to the Services (in whole or part) if: (a) Customer is in material breach (including non-payment); (b) required by law; (c) necessary to address a security risk; or (d) Customer's use threatens the availability or integrity of the Services. Where practicable, CIL will provide notice and an opportunity to cure.

15. Term, renewal, and termination

15.1 Term. This Agreement starts on the Effective Date and continues for the Subscription Term. The Subscription Term may renew as stated in the Order Form.

15.2 Termination for cause. Either Party may terminate an Order Form on written notice if the other Party materially breaches and fails to cure within 30 days of notice (or within 10 days for non-payment).

15.3 Immediate termination. Either Party may terminate immediately if the other becomes insolvent or ceases business.

15.4 Effect. On termination: (a) Customer's right to access ends; (b) Customer remains liable for Fees accrued; (c) upon request, CIL will make Customer Data available for export for 30 days

(unless legally prohibited). After that, CIL may delete Customer Data in accordance with the DPA and retention policy.

16. Compliance with laws

Each Party will comply with applicable laws in performing this Agreement, including data protection, anti-bribery, sanctions/export controls, and procurement rules where relevant.

17. Subcontracting

CIL may use subcontractors to perform the Services. CIL remains responsible for their performance. Where a subcontractor processes personal data, it will be appointed on terms consistent with the DPA.

18. Audit and records

If required by law or regulation applicable to Customer (e.g., public sector obligations), Customer may request reasonable information about CIL's security and compliance, including third-party audit reports (if available). On-site audits are permitted only by prior written agreement, limited to once per year, during business hours, and subject to confidentiality and security restrictions.

19. Notices

Notices must be in writing and delivered by hand, prepaid post, or email to the addresses stated in the Order Form (or as updated by notice). Notices are deemed received: (a) if by hand, on delivery; (b) if by post, two business days after posting; (c) if by email, at the time of sending provided no bounce-back is received.

20. General

20.1 Assignment. Neither Party may assign this Agreement without the other Party's prior written consent, except to an affiliate or in connection with a merger or sale of substantially all assets, provided the assignee agrees in writing to be bound.

20.2 Force majeure. Neither Party is liable for delay or failure caused by events beyond its reasonable control.

20.3 Entire agreement. This Agreement is the entire agreement and supersedes prior discussions.

20.4 No partnership. Nothing creates a partnership, joint venture, or agency.

20.5 Severability. If any provision is invalid, the remainder remains effective.

20.6 Governing law. This Agreement is governed by the laws of England and Wales and the courts of England and Wales have exclusive jurisdiction.



Schedule 1 – Order Form (Template)

Product/Service: TRAEMS

Customer: [Customer legal name]

Supplier: Ceucure Intelligence Limited

Effective Date: [●]

Initial Subscription Term: [e.g., 12 months]

Renewal: [auto-renew unless notice given 30 days prior / fixed term]

Subscription Plan: [●]

Authorised Users / Usage limits: [●]

Fees: [£●] [annual in advance / monthly]

Payment terms: [14 days]

Support level: [Standard / Premium]

Data residency (if applicable): [UK/EU/●]

Special terms: [●]

Signatures

For and on behalf of Ceucure Intelligence Limited	For and on behalf of Customer
Name: Title: Signature: Date:	Name: Title: Signature: Date:

Schedule 2 – Service Levels and Support

1. Support scope and channels

Support Hours (Standard): 09:00–17:00 UK business days (excluding UK public holidays) unless otherwise stated in the Order Form.

Support Channels: web ticketing and email. Phone support may be provided if included in the Order Form.

Scope: incident triage, diagnosis, workaround guidance, and bug fixes for issues attributable to the Services. Requests for configuration, consultancy, or customisation may be treated as Professional Services and may be chargeable.

Out of scope: issues caused by Customer environment, third-party services not supplied by CIL, unsupported browsers/devices, and unauthorised modifications.

2. Incident management process

2.1 Submission. Customer will submit incidents with sufficient detail (impact, steps to reproduce, screenshots/logs where applicable).

2.2 Classification. CIL will assign a severity level (P1–P4) based on impact and will keep Customer reasonably informed.

2.3 Customer obligations. Customer must provide reasonable cooperation, including timely responses to diagnostic requests and providing test access where necessary.

2.4 Escalation. Customer may request escalation through the designated support contact. Escalations are prioritised based on severity and impact.

3. Severity definitions and targets

Severity	Definition	Target first response	Target update cadence	Target workaround / resolution
P1	Critical outage or security incident; production unavailable or severe risk	15 Minutes	Every 2 hours	Quick Workaround: continuous effort until stabilised (24 Hours)
P2	Major impact; significant degradation; limited workaround	15 Minutes	Every 12 hours	Workaround within 5 business days where feasible; fix in next reasonable release

P3	Minor issue; workaround available	15 Minutes	Every 16 hours	Workaround within 7 business days
P4	Service request / how-to / minor defect	15 Minutes	Daily	Workaround within 10 business days
P5	Routine Maintenance / General Inquiry	15 Minutes	Bi-daily	Workaround within 12 business days

4. Availability (uptime)

4.1 Target. CIL will use commercially reasonable efforts to provide 99.9% monthly uptime for TRAEMS, excluding Permitted Downtime.

4.2 Permitted Downtime includes: (a) planned maintenance with reasonable notice; (b) emergency maintenance; (c) downtime caused by Customer systems, networks, or third-party services; (d) force majeure; and (e) suspension under the Agreement.

4.3 Measurement. Uptime is measured at the Service boundary as determined by CIL's monitoring systems, acting reasonably.

5. Service credits (if included)

5.1 Unless expressly included in the Order Form, service credits do not apply.

5.2 If included, credits are Customer's sole remedy for failure to meet uptime targets (excluding mandatory legal remedies).

5.3 Claim process. Customer must submit a claim within 30 days after the end of the month in which the failure occurred, including supporting evidence. Approved credits are applied to future invoices and are not refundable.

Schedule 3 – Acceptable Use Policy (AUP)

Customer and Authorised Users must not use the Services to:

- Violate any law or regulation (including data protection, export controls, or procurement rules).
- Transmit malware, exploit vulnerabilities, or interfere with the integrity or performance of the Services.
- Access or attempt to access accounts or data without authorisation.
- Send spam or unlawful marketing communications.
- Upload or distribute content that is defamatory, obscene, hateful, or infringes intellectual property rights.
- Conduct security testing (including penetration testing) without CIL's prior written consent.
- Process special category data or highly sensitive data unless expressly permitted in the Product Schedule and Order Form.
- Use the Service to make automated decisions producing legal or similarly significant effects about individuals without appropriate human review and lawful basis.

Schedule 4 – Security Measures

CIL will implement and maintain technical and organisational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. Measures include, as applicable:

- Governance: documented security policies; designated security ownership; periodic review of controls.
- Access control: role-based access; least privilege; MFA for administrative access; joiner/mover/leaver process; periodic access reviews for privileged accounts.
- Network security: segmentation of production environments; firewalling; secure remote access; protections against common web threats (e.g., rate limiting/WAF where appropriate).
- Encryption: TLS for data in transit; encryption at rest for production data stores where feasible; secure key management.
- Secure development: change management; code review practices; separation of duties for production changes; use of dependency scanning and security testing appropriate to the environment.
- Logging and monitoring: centralised logging for key security events; monitoring and alerting; audit trails for privileged actions where applicable.
- Vulnerability management: patching process; vulnerability triage and remediation; periodic scanning; coordinated disclosure handling.
- Backups and resilience: backups with defined retention; tested restore procedures; resilience planning; disaster recovery processes as appropriate to service tier.
- Physical and hosting security: use of reputable hosting providers; physical security controls managed by the hosting provider; environmental protections.
- Incident response: documented incident response plan; internal escalation; customer notification process as per the DPA.
- Supplier management: due diligence for key subprocessors; contractual security obligations flowed down.
- Data minimisation: access to Customer Data limited to personnel with a need to know for support/operations.
- Audit logging for privileged actions and exports of Workforce Data (where enabled).

Security commitments and customer responsibilities

Customer is responsible for: (a) enforcing strong passwords and MFA for its users where available; (b) controlling user provisioning; (c) securing endpoints and networks; and (d) configuring security options provided by the Services (e.g., meeting controls, export permissions).

Schedule 5 – Data Processing Addendum (UK GDPR / GDPR)

1. Definitions

1.1 “Data Protection Laws” means all applicable data protection and privacy laws and regulations, including the UK GDPR, the Data Protection Act 2018, the EU GDPR (where applicable), and any guidance or codes of practice issued by a competent authority.

1.2 “Personal Data”, “Processing”, “Controller”, “Processor”, “Data Subject”, “Supervisory Authority”, and “Personal Data Breach” have the meanings given in Data Protection Laws.

1.3 “Security Incident” means a confirmed Personal Data Breach involving Customer Personal Data processed under this Agreement.

2. Roles and scope

2.1 Relationship. Where CIL processes personal data on behalf of Customer in providing the Services, Customer is the Controller and CIL is the Processor, unless the Order Form states otherwise.

2.2 Instructions. CIL will process Customer Personal Data only on documented instructions from Customer, including as set out in this Agreement and Order Forms, unless required by law (in which case CIL will inform Customer unless prohibited).

3. Details of processing (Annex A)

The Parties acknowledge and agree the processing details below form Annex A to this DPA and may be supplemented by an Order Form.

Item	Description
Data subjects	Employees, contractors, workforce members, supervisors/managers.
Personal data categories	User profiles; contact details; role/department; schedules/rosters; time/attendance records; operational notes; audit logs.
Special category data	Not intended by default; may be included if Customer enters it. Customer must restrict and justify any special category processing.
Processing purpose	Workforce planning, scheduling, operational coordination, and reporting.
Data residency	As specified in Order Form (default: UK/EU hosting).

4. CIL (Processor) obligations

CIL will:

- Process Customer Personal Data only on Customer’s documented instructions (Section 2.2).

- Ensure persons authorised to process Customer Personal Data are subject to confidentiality obligations.
- Implement appropriate technical and organisational measures (Schedule 4) and maintain them during the Subscription Term.
- Taking into account the nature of processing, provide reasonable assistance to Customer to respond to Data Subject requests (access, deletion, rectification, objection, portability).
- Provide reasonable assistance to Customer with DPIAs and consultations with Supervisory Authorities where required, to the extent the relevant information is available to CIL and the request is reasonable.
- Notify Customer of a confirmed Security Incident without undue delay and, where practicable, within 72 hours after confirmation, providing information reasonably required by Customer to meet its notification obligations.
- At Customer's choice, delete or return Customer Personal Data at the end of the Services in accordance with Section 7 (Deletion/Return), unless retention is required by law.
- Make available information reasonably necessary to demonstrate compliance and allow audits as set out in Section 6 (Audit).

5. Subprocessing

5.1 General authorisation. Customer grants CIL general authorisation to appoint subprocessors to process Customer Personal Data for the purposes of providing the Services.

5.2 Flow-down. CIL will impose data protection obligations on subprocessors substantially equivalent to those in this DPA.

5.3 Changes. CIL will provide reasonable prior notice of material changes to subprocessors where practicable, allowing Customer to object on reasonable grounds relating to data protection. If the Parties cannot resolve the objection within 30 days, Customer may terminate the affected Services and receive a refund of prepaid Fees for the unused portion.

6. Audit

6.1 Documentation. Upon request, CIL will provide available information and, where applicable, third-party audit reports or summaries (if available) to demonstrate security and compliance.

6.2 On-site audit. On-site audits are permitted only as set out in Section 17 of the Agreement: by prior written agreement, limited to once per year, during business hours, and subject to confidentiality and security restrictions. Customer must use an independent auditor acceptable to CIL acting reasonably.

7. Deletion and return

7.1 During Subscription Term. Customer may export Customer Data using Service functionality (where available).

7.2 End of Services. Following termination or expiry, CIL will make Customer Data available for export for 30 days (unless legally prohibited). After that, CIL will delete Customer Personal

Data from production systems within a reasonable period, subject to backup retention cycles and legal retention requirements.

7.3 Backups. Customer Personal Data may persist in backups for a limited period consistent with backup retention policies, after which it will be deleted in the ordinary course.

8. International transfers

8.1 Transfers. Where Customer Personal Data is transferred outside the UK and/or EEA, CIL will ensure appropriate safeguards as required by Data Protection Laws.

8.2 Safeguards. Such safeguards may include the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, and/or the EU Standard Contractual Clauses (as applicable). The Parties will execute transfer documentation upon request where required.

9. Liability

The limitations and exclusions of liability in the Agreement apply to this DPA to the maximum extent permitted by law.

Annex B – Subprocessors (template)

CIL will maintain a current list of subprocessors used to provide the Services. The list may be provided on request or via a published subprocessor page. At minimum, the following information should be recorded:

Subprocessor	Service	Processing location(s)	Purpose
[•]	[Hosting / Email / Analytics / Support]	[UK/EU/•]	[•]
[•]	[Hosting / Email / Analytics / Support]	[UK/EU/•]	[•]
[•]	[Hosting / Email / Analytics / Support]	[UK/EU/•]	[•]

Schedule 6 – Product Schedule: TRAEMS

Service description and scope

The Service supports workforce scheduling/rostering, shift management, workforce operations workflows, reporting, and audit logs.

Customer is responsible for configuration of roles, approval flows, pay rules (if applicable), and operational policies.

No employment-law compliance guarantee

Customer acknowledges that workforce rules and employment/union obligations vary by jurisdiction and organisation. The Service provides tools to configure schedules and rules but does not constitute legal advice and does not guarantee compliance with employment law, collective agreements, or internal policies.

Customer is responsible for verifying outputs (including overtime, rest periods, and approvals) and for ensuring appropriate approvals and governance are in place.

Integrations (payroll/HR/identity)

If the Service integrates with payroll, HRIS, identity providers, or messaging tools, such integrations must be specified in the Order Form. CIL does not warrant the availability of third-party APIs or services.

Operational and safety considerations

Customer is responsible for ensuring that schedules and operational decisions created using the Service are reviewed and are fit for purpose, especially where they affect safety-critical staffing or emergency coverage.