

These terms and conditions ("Terms") govern the use of cloud-based software services ("Services") provided by Cognitas Global Ltd a company registered in England under registration number 11700911 whose registered office is at Suite 2078, Fleet House Springhead Enterprise Park, Springhead Road, Northfleet, Kent DA11 8HJ a company registered in England & Wales (hereinafter referred to as "Cognitas Global") ("Company"), to the user ("User" or "You") internationally. By accessing or using the Services, you agree to be bound by these Terms. If you do not agree to these Terms, do not access or use the Services.

1. Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following terms have the meanings set out below:

(a) "Agreement" means this Master Subscription Agreement together with the Schedules, Annexes, Service Terms, and any Order Form(s) entered into between the parties.

(b) "Customer" means the contracting public sector body, governmental authority, arm's-length agency, or other entity procuring the Service under this Agreement.

(c) "Customer Data" means data, information, documents, records, submissions, logs, decisions, narrative content, assessments or other materials input by or on behalf of Customer or its Users during the use of the Service.

(d) "Effective Date" means the date on which this Agreement is executed by both parties, or the date of the relevant Order Form, whichever is earlier.

(e) "Order Form" means a document executed by the parties that specifies the Subscription(s) purchased, term, Fees, and any applicable Professional Services.

(f) "Professional Services" means scenario customisation, facilitation, exercise delivery, content adaptation, training, consultancy, or other services provided by Supplier that are distinct from the Subscription to the Service.

(g) "Service" means the View360Global cloud-based experiential learning and exercising platform, and any associated modules made available by Supplier to Customer under this Agreement.

(h) "Subscription" means a right to access and use the Service during the Term, subject to the scope restrictions set out in this Agreement and in the applicable Order Form.

(i) "Supplier" means Cognitas Global Ltd, a company registered in England and Wales with company number 11700911 and registered address at Suite 2087, Fleet House, Springhead Road, Northfleet, Kent DA11 8HJ.

(j) "Term" means the duration of this Agreement as set out in Clause 10.

(k) "User" means an individual member of Customer (or authorised third-party participant, as applicable) who is permitted to access or use the Service pursuant to this Agreement.

1.2 Headings are for convenience only and shall not affect interpretation.

1.3 Words importing the singular include the plural and vice versa.

1.4 In the event of conflict, the following order of precedence applies:

- (a) Order Form(s)
- (b) Schedules and Annexes
- (c) SaaS Service Terms (Part 2)
- (d) this Master Subscription Agreement (Part 1)
- (e) Support & SLAs (Schedule)
- (f) Pricing Catalogue (Schedule)

2. Appointment and Scope

2.1 Customer engages Supplier to provide the Service on a Subscription basis, together with any Professional Services ordered.

2.2 The parties acknowledge that this Agreement applies to the View360Global platform and does not include the supply of hardware, networks, client devices, or telecommunications infrastructure.

2.3 Customer remains responsible for meeting its own internal security, operational, governance and compliance requirements and for its own data stewardship obligations.

3. Subscription Licence Grant

3.1 Subject to Customer's compliance with this Agreement and payment of Fees, Supplier grants to Customer a non-exclusive, non-transferable, non-sublicensable right to access and use the Service during the Term for Customer's internal organisational purposes.

3.2 The Subscription does not include ownership of the Service, software, platform, modules, scenarios, templates, frameworks, injects, media, audio-visual content, analytics tools, or any other intellectual property of Supplier.

3.3 The Subscription is provided on a cloud/SaaS basis only. No software shall be provided for installation by Customer.

4. Restrictions on Use

4.1 Customer shall not:

- (a) sub-licence, rent, lease, transfer, distribute or commercially exploit the Service;
- (b) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code;

- (c) remove or alter proprietary notices; or
- (d) use the Service to provide training-as-a-service to third parties without Supplier's prior written consent.

4.2 Customer shall ensure Users comply with this Agreement.

5. Fees and Charges

5.1 Subscription Fees and Professional Services Fees are set out in the applicable Order Form or Pricing Catalogue.

5.2 Fees shall be payable in GBP or EUR, as set out in the Order Form, and exclusive of VAT.

5.3 Subscription Fees are non-refundable except as expressly stated.

5.4 Non-payment may result in suspension of access to the Service.

6. Customer Responsibilities

6.1 Customer is responsible for:

- (a) provisioning Users;
- (b) verifying User authorisation;
- (c) ensuring Users comply with acceptable use policies; and
- (d) the accuracy, legality and integrity of Customer Data.

6.2 Customer shall not use the Service to store or transmit:

- (a) harmful code;
- (b) content infringing the rights of others; or
- (c) operational real-world incident traffic unless anonymised, redacted or simulated.

6.3 Customer acknowledges that exercises delivered via the Service are simulation/learning environments and shall not be used as a substitute for operational communications systems.

7. Supplier Responsibilities

7.1 Supplier shall provide the Service in accordance with this Agreement and applicable laws.

7.2 Supplier shall ensure that the Service materially conforms to the description in the Service Definition and Pricing Catalogue.

7.3 Supplier may modify the Service provided such modifications do not materially diminish core functionality.

8. Confidentiality

8.1 Each party shall keep confidential the Confidential Information of the other.

8.2 Confidentiality obligations survive termination for five (5) years.

8.3 Confidentiality does not apply to information that is public, independently developed, or lawfully disclosed by a third party.

9. Intellectual Property

9.1 Ownership of intellectual property is addressed in the IP Schedule (Part 4).

9.2 Nothing in this Agreement transfers ownership of Supplier IP or Customer Data.

10. Term and Renewals

10.1 This Agreement begins on the Effective Date and continues for the Initial Term set out in the Order Form.

10.2 Unless terminated, Subscriptions will automatically renew for Renewal Terms on the then-current Fees, unless either party gives ninety (90) days' notice.

11. Termination

11.1 Either party may terminate for material breach not remedied within thirty (30) days.

11.2 Either party may terminate if the other becomes insolvent.

11.3 Upon termination:

(a) Customer access shall cease;

(b) Customer Data shall be handled per the Exit and Data Retention Schedule.

12. Notices

12.1 Notices shall be in writing and delivered by email or registered mail.

12.2 Notices to Supplier shall be delivered to:

Cognitas Global Ltd, Suite 2087, Fleet House, Springhead Road, Northfleet, Kent DA11 8HJ.
Attention: CEO

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of England and Wales.

13.2 The courts of England and Wales have exclusive jurisdiction.

14. Service Provision and Access

14.1 Supplier shall provide the Service via secure remote access over the internet.

14.2 Customer acknowledges that the Service is cloud-hosted and delivered as software-as-a-service (SaaS), and no software code is delivered for installation by Customer.

14.3 Supplier shall make the Service available to Customer Users during the Term, subject to scheduled and emergency maintenance as permitted under Clause 17.

15. User Accounts and Authentication

15.1 Customer is responsible for issuing and managing User accounts in accordance with Supplier's access control processes.

15.2 Customer shall ensure that Users maintain secure credentials and do not share access between individuals.

15.3 Customer shall promptly notify Supplier if it suspects a compromise of User credentials.

16. Customer Data Input and Use

16.1 Customer retains all rights, title and interest in Customer Data.

16.2 Customer is solely responsible for ensuring that Customer Data is lawful, accurate and suitable for processing in connection with the Service.

16.3 Supplier does not monitor, validate or verify Customer Data; however, Supplier may remove content that it reasonably determines to be unlawful or in violation of this Agreement.

16.4 Customer Data shall not include personal data beyond what is necessary for the performance of the Service. Personal data processing is governed by the Data Processing Agreement.

17. Maintenance and Service Modifications

17.1 Supplier may perform scheduled maintenance outside normal working hours or at times reasonably designed to minimise disruption.

17.2 Supplier may implement emergency maintenance as required for security or service integrity reasons.

17.3 Supplier may modify, update or enhance the Service, provided that such changes do not materially degrade core functionality.

18. Service Availability

18.1 Supplier shall use reasonable commercial efforts to provide Service availability in accordance with the Service Levels set out in Schedule (SLAs).

18.2 Service availability shall exclude maintenance windows, emergency maintenance, service provider outages, force majeure events, or failures attributable to Customer systems or networks.

19. Support and Ticketing

19.1 Supplier shall provide support services as described in the Support Schedule, including incident management and technical ticketing.

19.2 Incident response targets shall be reasonable and proportionate to incident severity.

20. Third-Party Providers and Subprocessors

20.1 Supplier may engage third-party cloud providers, hosting services or subprocessors for the delivery of the Service.

20.2 Supplier shall remain responsible for the performance of subprocessors under this Agreement.

20.3 Subprocessors shall be identified in the Data Processing Agreement.

21. Acceptable Use

21.1 Customer and Users shall not use the Service to:

- (a) perform unauthorised penetration testing or security scanning;
- (b) deploy malware, harmful code or operational command traffic;
- (c) simulate live operational emergencies without appropriate redaction or abstraction;
- (d) undertake actions likely to compromise the integrity of the Service or other Customer environments;
- (e) violate applicable law or third-party rights.

21.2 Supplier may suspend or restrict access for material breach of acceptable use.

22. Simulation, Exercising and Training Context

22.1 Customer acknowledges that the Service is designed for training, exercising and learning purposes.

22.2 The Service is not intended to replace operational command-and-control systems, emergency communications systems, crisis communications platforms, or other safety-critical operational environments.

22.3 Exercises run on the Service may involve realistic but abstracted content and shall not be relied upon for live operational decision-making.

23. Multi-Party and Co-Facilitation Use Cases

23.1 The Service may support scenarios, simulations or exercises involving multiple customer stakeholders or departments.

23.2 Where multi-party participation occurs, each party shall remain responsible for its own Users and Data.

23.3 Co-facilitation or professional services components shall be addressed in the Professional Services Schedule.

24. Data Protection – Roles and Responsibilities

24.1 For the purposes of UK and EU data protection legislation, Customer shall be the “Controller” of personal data processed through use of the Service, and Supplier shall act as the “Processor”, except where Supplier processes data for its own administration, billing, or account management purposes, in which case Supplier shall act as an independent Controller.

24.2 Customer warrants that it has obtained all necessary consents, authorisations and lawful bases to permit the processing of personal data via the Service.

24.3 Supplier shall process personal data solely for the purpose of providing the Service and in accordance with Customer's documented instructions as set out in this Agreement and any Order Form.

25. Data Processing Agreement (DPA)

25.1 A Data Processing Agreement shall apply to the processing of personal data and forms a binding part of this Agreement.

25.2 The DPA incorporates (as applicable):

- (a) UK GDPR and Data Protection Act 2018;
- (b) EU GDPR (if Customer is located in an EU jurisdiction);
- (c) any mandatory guidance issued by the UK ICO or European Data Protection Board; and
- (d) standard contractual clauses or international transfer mechanisms where applicable.

25.3 If there is inconsistency between this Agreement and the DPA, the DPA shall prevail with respect to personal data.

26. Data Security and Technical Measures

26.1 Supplier shall implement and maintain appropriate technical and organisational measures to protect Customer Data, including measures relating to:

- (a) encryption at rest and in transit;
- (b) access control and authentication;
- (c) logging and monitoring;
- (d) vulnerability management and patching;
- (e) incident response; and
- (f) segregation of customer data.

26.2 Supplier shall implement data minimisation principles and shall not access Customer Data except as necessary for support or to comply with law.

27. Subprocessors

27.1 Supplier may engage subprocessors for hosting, storage or service provision, subject to the DPA.

27.2 Supplier shall maintain a list of subprocessors and notify Customer of material changes.

27.3 Supplier remains liable for the acts and omissions of subprocessors.

28. Security Standards and Compliance

28.1 Supplier shall use commercially reasonable efforts to operate the Service in alignment with relevant security frameworks applicable to UK public sector buyers, including NCSC principles applicable to cyber exercising and training environments.

28.2 Nothing in this Agreement obligates Supplier to achieve formal certification unless expressly agreed in writing.

29. Security Incidents

29.1 Supplier shall notify Customer without undue delay upon becoming aware of a confirmed personal data breach affecting Customer Data.

29.2 Notifications shall include reasonable information to assist Customer in meeting its regulatory obligations.

29.3 Customer shall remain solely responsible for regulatory notifications except where Supplier is required by law to notify a regulator.

30. Customer Security Responsibilities

30.1 Customer is responsible for:

- (a) managing internal access controls;
- (b) managing User credential hygiene;
- (c) assessing learning and exercising environments for classification restrictions; and
- (d) ensuring appropriate redaction, anonymisation, or abstracting of sensitive operational content.

30.2 Customer acknowledges that simulation environments are not designed to handle classified, operationally sensitive, or “SECRET” information unless separately agreed in a secure enclave.

31. Data Portability and Export

31.1 Customer may export Customer Data during the Term in a common format, subject to reasonable technical safeguards.

31.2 Export tools may include CSV, JSON, PDF, or equivalent structured data formats.

31.3 Supplier shall not impose data export charges except for reasonable Professional Services where bespoke export formats are requested.

32. Data Retention and Deletion

32.1 Upon termination or expiry, Customer Data shall be retained for a limited period for extraction, subject to Clause 33.

32.2 Following the retention period, Supplier shall delete Customer Data in accordance with the Exit and Data Retention Schedule.

33. Exit Model (Option 1 – Customer Retains + Supplier Deletes)

33.1 Upon termination, Customer shall retain Customer Data and Supplier shall permanently delete Customer Data after a defined extraction period.

33.2 Supplier shall not retain Customer Data beyond the extraction period, except as required by law.

33.3 This clause does not restrict Supplier's retention of billing data, contractual records, or anonymised statistics unrelated to Customer Data.

34. Data Localisation and International Transfers

34.1 Supplier may store or process data in the UK, EEA or other jurisdictions that ensure adequate safeguards under applicable data protection laws.

34.2 International transfers requiring SCCs or equivalent mechanisms shall be governed by the DPA.

35. Data Categories for Exercising and Simulation

35.1 The parties recognise that exercising environments may involve:

- (a) participant responses, decisions and logs;
- (b) simulated events, injects or scenario content; and
- (c) abstracted operational information.

35.2 Customer warrants that data used for exercising purposes shall be suitably abstracted or redacted to avoid disclosure of classified operational traffic unless otherwise agreed.

36. Freedom of Information (FOI) and Public Sector Requests

36.1 Customer acknowledges that it may be subject to FOIA or equivalent.

36.2 Supplier shall support Customer in responding to FOI requests but shall not be required to disclose Supplier Confidential Information, trade secrets, platform IP, or commercially sensitive information.

37. Intellectual Property – General

37.1 Except as expressly provided in this Agreement, nothing transfers ownership of any intellectual property rights (“IPR”) between the parties.

37.2 Supplier retains all right, title and interest in Supplier IP, including:

- (a) the View360Global platform;
- (b) scenario engines, branching logic and simulation frameworks;
- (c) inject sequencing and timeline tools;
- (d) templates, playbooks and multimedia assets;
- (e) analytics modules, reporting formats and visualisations;
- (f) design language and UI/UX components;
- (g) documentation, training materials and facilitation guides; and
- (h) derivative improvements or enhancements.

37.3 Customer retains all right, title and interest in Customer IP, including:

- (a) Customer Data;
- (b) internal learning artefacts and outputs;
- (c) decisions, logs, assessments and reflections generated during exercises;
- (d) organisational knowledge or operating models disclosed during exercises.

38. Scenario Content and Exercising IP (A + B Models)

38.1 Supplier-Owned Scenario IP (**Model A**)

Supplier retains ownership of pre-built scenarios, scenario templates, inject sets, multimedia injects, and simulation content developed independently of Customer.

38.2 Joint IP for Co-Developed Content (**Model B**)

Where Customer contributes organisational materials, regulatory context, SOPs, incident data, practices or workflows to produce a tailored scenario, such scenario shall constitute **Joint IP** to the extent of each party’s contributions.

38.3 Customer-Contributed Content

Customer retains ownership of Customer-contributed organisational materials used in tailoring

and shall grant Supplier a non-exclusive licence to use such materials for delivery of exercises to Customer.

38.4 Use of Joint Scenario IP

(a) Customer may use Joint IP for internal training and exercising.

(b) Supplier may use Joint IP for scenario delivery to Customer and for internal product improvement, provided identifiable Customer Confidential Information is removed or anonymised.

38.5 No Crown IP Claim

Nothing in this Agreement transfers Supplier's platform scenario IP to Crown ownership unless agreed in writing via a Crown IP clause (not applicable by default under CCS Cloud Lots).

39. Exercise Outputs and Auditability

39.1 Customer owns all decision logs, outcomes, assessments, reflections, and exercise outputs created during scenario execution.

39.2 Supplier may retain anonymised aggregate analytics for product improvement and benchmarking, provided no Customer Confidential Information or personal data is disclosed.

40. Professional Services IP

40.1 Professional Services that involve scenario customisation, facilitation or exercising do not transfer platform IP.

40.2 Deliverables produced as part of Professional Services shall be licensed for Customer's internal use only.

41. Feedback and Improvement Rights

41.1 Customer may provide feedback relating to the Service.

41.2 Supplier may use such feedback without restriction for improvement, provided no Customer Confidential Information is disclosed.

42. Third-Party IP and Licensing

42.1 Where third-party content is incorporated into the Service (e.g., video, media, regulatory frameworks), such content remains subject to third-party IPR and licensing.

42.2 Customer is responsible for ensuring it has rights to contribute third-party content to exercises.

43. Exit and Post-Termination Assistance

43.1 Upon termination or expiry, Customer's Subscription shall cease and the Exit Model under Clause 33 shall apply.

43.2 Supplier shall provide reasonable assistance for data extraction during the extraction period.

43.3 Professional Services for extended exit assistance may be chargeable at rates specified in the Pricing Catalogue.

44. Retention and Deletion

44.1 Supplier shall retain Customer Data only for the extraction period.

44.2 After such period, Supplier shall permanently delete Customer Data, subject to legal retention obligations under Clause 45.

45. Legal Retention Requirements

45.1 Supplier may retain records strictly limited to billing, contractual, operational, or regulatory compliance purposes, provided such records contain no Customer Data except as required by law.

46. Warranties

46.1 Supplier warrants that the Service shall materially conform to the Service Description during the Term.

46.2 Supplier disclaims implied warranties to the maximum extent permitted by law.

46.3 The Service is provided for simulation, training and exercising, and shall not be used for operational emergency communications or safety-critical systems.

47. Indemnities

47.1 Supplier shall indemnify Customer against third-party claims alleging that the Platform infringes third-party IPR, provided Customer:

- (a) notifies Supplier promptly;
- (b) provides reasonable cooperation; and
- (c) allows Supplier sole defence control.

47.2 Supplier shall have no liability for claims arising from:

- (a) Customer modifications;
- (b) third-party content;
- (c) Customer-contributed training content; or
- (d) Customer's breach of this Agreement.

47.3 Customer shall indemnify Supplier against claims relating to Customer Data submitted or used during exercises.

48. Liability

48.1 Liability shall be subject to the limitations in this Clause 48.

48.2 Liability for death or personal injury caused by negligence, fraud, or other liabilities that cannot be excluded by law shall not be limited.

48.3 Neither party shall be liable for indirect, consequential, special or punitive damages.

48.4 Supplier's aggregate liability under this Agreement shall not exceed the Fees paid by Customer in the twelve (12) months preceding the claim.

48.5 The parties acknowledge that simulation and exercising environments may produce behavioural outputs and reflection data, and Supplier shall not be liable for Customer decisions based on such outputs.

49. Insurance

49.1 Supplier shall maintain reasonable insurance coverage customary for SaaS and Professional Services providers, including public liability and professional indemnity.

50. Force Majeure

50.1 Neither party shall be liable for delays or failure to perform caused by events beyond its reasonable control.

51. Dispute Resolution

51.1 The parties shall use reasonable endeavours to resolve disputes amicably before resorting to litigation.

Schedules

Schedule 1 — Pricing & Catalogue Structure

1. Overview

1.1 Pricing under this Agreement follows a **Hybrid Catalogue Model**, comprising:

- (a) SaaS Subscription Fees (View360Global Platform)
- (b) Cohort/Exercise Delivery Fees
- (c) Professional Services Fees
- (d) Training & Enablement
- (e) Optional Modules (where applicable)

1.2 Pricing is exclusive of VAT and taxes.

2. SaaS Subscription Fees

Subscription Fees may be structured as:

- (a) per-user or named-user basis;
- (b) per-group or organisational licence; or
- (c) enterprise licence.

Catalogue structure may include:

- Annual Subscription Fee
- Platform Access
- Facilitator and Admin Seats
- Viewer/Observer Seats
- Scenario Library Access (where applicable)

3. Exercise & Cohort Delivery Fees

3.1 Delivery Fees may apply to:

- (a) Tabletop Exercises (TTX)
- (b) Scenario-based Simulation
- (c) Multi-party Exercises
- (d) Professional Facilitation
- (e) Co-Facilitation with Customer

3.2 Delivery Fees may be priced on a:

- (a) per-cohort basis; or
- (b) day-rate basis.

Both models are permissible under G-Cloud.

4. Professional Services Fees

Professional Services may include:

- Scenario Development
- Scenario Adaptation
- Sector Tailoring
- Consulting
- Training & Enablement
- Learning & Evaluation
- Content Localisation
- Workshop Facilitation

Fees may be day-rate based or flat-fee based.

5. Optional Modules and Add-ons

Optional modules shall not form part of the evaluated price unless expressly requested. Optional modules may include:

- Advanced Analytics & Reporting
- Certification & Recognition
- Capacity Transfer Module
- Coaching & Triads
- Leadership Development Components
- Scenario Packs (Sector-specific)
- AI/Automated Insight Tools (if available)

6. Payment Terms

6.1 Payment shall be Net 30 unless otherwise agreed in the Order Form.

6.2 Annual Subscriptions are billed in advance.

6.3 Professional Services are billed monthly in arrears or on milestone completion.

7. Currency

Fees shall be payable in GBP or EUR, as set out in the Order Form.

Schedule 2 — Professional Services Scope

1. Description

Professional Services are optional and separate from SaaS Subscriptions. Services may include:

- (a) Exercise design, adaptation and delivery
- (b) Scenario tailoring to Client context
- (c) Facilitation & co-facilitation
- (d) Training & enablement
- (e) Advisory & consultancy
- (f) Project management
- (g) Evaluation, reflection and learning support

2. Delivery Model

Professional Services may be delivered:

- (a) remotely, via View360Global and virtual conferencing; or
- (b) in person, at mutually agreed locations.

Remote delivery is standard for G-Cloud.

3. Acceptance Criteria

Professional Services are deemed accepted upon delivery unless disputed in good faith within ten (10) days.

Schedule 3 — Support & Service Levels (SLAs)

1. Service Support

Supplier shall provide support as follows:

- Technical Ticketing

- Incident Response
- Troubleshooting
- User Support

2. Service Availability

Availability targets are for reference and do not constitute warranties:

- Platform Availability Target: **99.5%** (excluding maintenance windows)

3. Incident Severity Levels

Incidents shall be categorised as follows:

- **Severity 1 (Critical):** Platform unavailable
- **Severity 2 (Major):** Material functionality degraded
- **Severity 3 (Minor):** Non-critical issue
- **Severity 4 (Informational):** Non-impact issue or request

4. Maintenance Windows

- Scheduled Maintenance: outside business hours
- Emergency Maintenance: as required for security or stability

Schedule 4 — Definitions & Interpretation

The following definitions apply to this Agreement:

“Confidential Information” has the meaning set out in Clause 8.

“Customer Data” has the meaning set out in Clause 16.

“Joint IP” means scenario content developed collaboratively by the parties.

“Order Form” means the document specifying Subscription and Fees.

“Professional Services” has the meaning set out in Schedule 2.

“Service” has the meaning set out in Clause 1.

“Subscription” means the right to access the Service.

“Supplier” means Cognitas Global Ltd.

“Term” means the duration described in Clause 10.

“User” means authorised Customer personnel.

Schedule 5 — Entire Agreement Clause

This Agreement constitutes the entire agreement between the parties and supersedes all prior proposals, negotiations or understandings relating to the Service.

Schedule 6 — Signatures

Supplier:

Cognitas Global Ltd

Suite 2087, Fleet House, Springhead Road, Northfleet, Kent DA11 8HJ

Signature: _____

Name: _____

Role: CEO

Date: _____

Customer:

[Public Sector Customer Name]

[Address]

Signature: _____

Name: _____

Role: _____

Date: _____