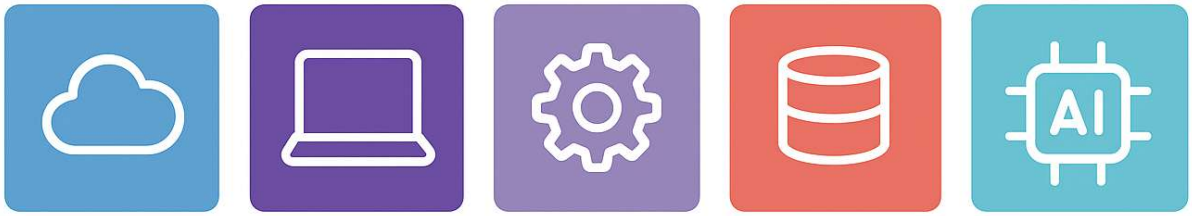
Chris Johnson Studio LTD Terms & Conditions (Supplier Supplement)

Framework: G-Cloud 15 • Lot 3: Cloud Support
Service Definition: Cloud Application Support, DevOps and AI Enablement
Supplier: Chris Johnson Studio Ltd (CJS)
Date: 16/11/2025



Important precedence note:
If there is any conflict or ambiguity between these Supplier Supplemental Terms and the CCS G-Cloud 15 Framework and/or the applicable Call-Off Contract (including the Order Form and incorporated Schedules), the Framework and Call-Off terms take precedence.

Contact:

Christopher Johnson, Managing Director
Email: chris@chrisjohnsonstudio.com
Web: www.chrisjohnsonstudio.com
Address: 4 Longmeadow, Beckington, Somerset, BA11 6BA

1. Definitions

“Agreement” means the Call-Off Contract between the Buyer and CHRIS JOHNSON Studio LTD (the “Supplier”), including these Supplemental Terms and all schedules/annexes.
“Buyer” means the public sector Customer named in the Call-Off Contract.
“Confidential Information” means all information identified as confidential or that reasonably should be considered confidential.
“Deliverables” means all materials specifically produced for the Buyer as described in the Order Form.
“Digital Marketplace Listing” means the Supplier’s service listing on the G-Cloud Digital Marketplace, as updated from time to time.
“Order Form” means the Call-Off order form signed or accepted by the parties via the CCS portal.
“Personal Data”, “Controller”, “Processor”, “Data Subject”, “UK GDPR” have the meanings given in applicable data protection laws.
“Services” means the cloud support and related services described in the Order Form and Service Definition.
“SLA” means the service levels set out in Schedule 2.

2. Scope of Services

2.1 The Supplier shall provide the Services described in the Order Form, Service Definition and Digital Marketplace Listing.
2.2 Associated services (training, documentation, onboarding, DevOps, CI/CD, incident response and monitoring) shall be provided where specified.
2.3 Bespoke application design/development and greenfield product builds are out of scope of this listing and may be contracted separately under a Call-Off/SoW.”
2.4 Any works not expressly set out are out of scope unless added through the Change Control procedure in Section 10.

3. Term and Renewal

3.1 Commencement and Initial Term. The Agreement starts on the Commencement Date stated in the Order Form and continues for the Initial Term

specified therein, unless ended earlier in accordance with Section 19 or the applicable Call-Off terms.

3.2 No automatic renewals. The Agreement does not automatically renew. Any extension or renewal must be expressly agreed via the CCS G-Cloud Call-Off process (by Call-Off variation or new Call-Off) before expiry and in accordance with the Framework and Call-Off terms.

3.3 Optional extensions (if stated). Where the Order Form identifies optional extension period(s), the Buyer may, at its sole discretion, exercise such extension(s) via the CCS G-Cloud Call-Off process before expiry. No extension applies unless and until confirmed in writing through that process.

3.4 Renewal planning (non-binding). To support continuity of service where renewal is contemplated, the parties will aim to agree renewal plans in good time ahead of expiry (Supplier recommendation: at least eight months prior to end of term). This planning is non-binding and does not create a commitment to renew.

3.5 Expiry. If no extension or renewal is agreed before expiry, the Agreement ends at the end of the Initial Term (or then-current extension), and the Supplier will provide Exit and Off-boarding in accordance with Section 20.

4. Charges and Payment

4.1 Charges are as set out in the Order Form and/or Rate Card (Schedule 1). Unless otherwise stated, Charges are time-and-materials plus approved Expenses at cost.
4.2 Invoicing is monthly in arrears. Payment terms are 30 days net from receipt of a valid invoice.
4.3 Late payment may, at the Supplier’s discretion and subject to the Late Payment of Commercial Debts regime, accrue interest.
4.4 All Charges exclude VAT (or relevant sales tax) which shall be added where applicable.
4.5 The Buyer shall not unreasonably withhold or delay approval of time records or Deliverables.

5. Service Levels and Service Credits

5.1 Overview. Service Level Agreements (SLAs) are agreed per engagement and matched to the Buyer's chosen support level. Standard support hours are 09:00–18:00 UK, Monday–Friday (on-call available by agreement). Performance is measured monthly and reported in service reviews.

5.2 Severity definitions (guide).

- **P1 Critical:** full service outage or severe degradation with major user impact; no workaround.
- **P2 High:** significant impact or degraded service; workaround exists.
- **P3 Normal:** minor impact incident or routine service request.

5.3 Response targets (by support level).

- **Bronze:** P1 1 hour, P2 4 hours, P3 1 business day.
- **Silver:** P1 30 minutes, P2 2 hours, P3 8 hours.
- **Gold:** P1 15 minutes, P2 1 hour, P3 4 hours.

5.4 Availability targets (managed environments).

- ***Bronze:*** *99.5% • Silver: 99.9% • Gold: 99.95% — measured over the calendar month.*
- *Availability is measured at the service/application boundary operated by the Supplier and excludes planned maintenance and other agreed exclusions (see 5.10).*

5.5 Service desk performance. At least 95% of tickets receive a first human response within the applicable SLA each month.

5.6 Maintenance notifications.

- **Planned maintenance:** at least 48 hours' notice, scheduled outside business hours where possible.
- **Urgent security maintenance:** notified as soon as practicable; the aim is 24 hours' notice where risk allows.
- **Emergency maintenance:** commenced immediately with incident-style updates.

5.7 Service Credits (availability shortfall). If monthly availability falls below the agreed target for the chosen support level, a credit is applied to that month's managed-service fee as follows:

- Shortfall **≤ 0.5 percentage points:** 2.5% credit
- **> 0.5 to 1.0 pp:** 5% credit
- **> 1.0 to 2.0 pp:** 10% credit
- **> 2.0 pp:** 15% credit

5.8 Service Credits (response KPI). If the ≥95% first-response KPI in 5.5 is not met in a month, an additional 5% credit applies (only one response-time credit may apply per month).

5.9 Monthly caps and scope.

- **Caps:** Bronze 15%, Silver 20%, Gold 25% of that month's managed-service fee.
- **Scope:** Credits apply only to the fixed monthly fees for the managed environment/service under this listing; they do not apply to time-and-materials work, project services, third-party pass-through charges, or Buyer-caused delays.

5.10 Exclusions. Credits do not apply where breach is caused by: Buyer actions/approvals or change freezes; third-party or upstream provider outages outside contracted scope; force majeure; security incidents caused by Buyer-controlled credentials; or maintenance performed within agreed windows/urgent security timelines.

5.11 Measurement.

- **Availability** is calculated over the calendar month for the in-scope service, excluding periods defined in 5.10 and agreed maintenance windows.
- **Response performance** is measured from ticket receipt to first qualified human response.

5.12 Process. Preliminary credits are indicated in the monthly service report. The Buyer may submit a claim within 10 business days of report receipt; verified credits are applied to the next invoice (or refunded by agreement). Service Credits are an exclusive remedy and not a penalty.

5.13 Chronic failure. If credits at the monthly cap occur in two consecutive months or three in any six-month period, the Buyer may require a service improvement plan and/or exercise contractual remedies as set out in the Order Form/framework.

---

6. Ordering, Onboarding and Acceptance

6.1 Ordering.
Services commence on execution of an Order Form/Call-Off specifying scope, support level (Bronze/Silver/Gold), roles/rates, start date, and any minimum monthly commitment.

6.2 Mobilisation.
Within 5 working days (or as agreed) the Supplier schedules a kick-off, confirms points of contact and escalation, and agrees the initial plan and change windows.

6.3 Onboarding deliverables.
The Supplier will provide and/or agree:

- **Access setup & IAM** (least-privilege), environment onboarding and secrets handling.
- **Runbooks & support workflows** (incident, request, change), including ticketing routes and update cadence.
- **Target architecture & security/DR checkpoints** relevant to the service scope.
- **Monitoring/alerting dashboards** and initial thresholds.
- **Initial optimisation backlog** (cost, performance, resilience).
- **Training & knowledge transfer plan** appropriate to the Buyer team(s).

6.4 Dependencies and Buyer inputs.
Buyer provides timely access/approvals, nominated owners for sign-off, change-freeze dates, and any required policies (e.g., data residency, retention, security baselines).

6.5 Acceptance criteria.
Unless otherwise agreed in the Order Form, onboarding is accepted when:
(a) access/IAM and ticketing are live;
(b) runbooks and escalation paths are delivered;
(c) monitoring/alerts are active;
(d) initial optimisation backlog is agreed; and
(e) a kick-off/training session has been completed.
Where a migration/transition is in scope, additional acceptance is the successful completion of the agreed cutover and smoke tests.

6.6 Changes during onboarding.
Any material changes to scope, support level or timelines follow change control and are priced per Schedule 1. Emergency changes use the expedited path with Buyer approval.

6.7 Alignment to SLAs.
Operational SLAs and maintenance notice periods apply per Schedule 2 from the point the production environment is onboarded (or as otherwise stated in the Order Form).

6.8 Change freezes and expedited security changes.
Buyer change-freeze periods will be respected; urgent security updates may proceed following Buyer approval via the expedited change process. The Supplier will document the impact assessment, rollback plan and communications for any expedited change and include the activity in the monthly service report.

7. Buyer Responsibilities

7.1 General. The Buyer will provide timely inputs and approvals to enable safe, efficient delivery of the Services.

7.2 Access and approvals.

- Grant and maintain required environment access (least-privilege).
- Provide decision-maker availability and change-window approvals.
- Nominate escalation contacts and a service owner for sign-off.

7.3 Policies and governance.

- Supply applicable security, data protection, data residency/retention, and accessibility policies.
- Confirm any change freezes, release gates, or assurance steps (e.g., CAB).

7.4 Third-party dependencies.

- Ensure Buyer-managed and third-party systems, licences and integrations are available and supported; notify Supplier of constraints and maintenance.
- Manage commercial relationships with cloud/SaaS providers unless otherwise agreed.

7.5 Data and compliance.

- Determine Controller/Processor roles, lawful basis and retention; provide DPIAs where required.
- Approve sub-processors where needed and review evidence packs on request.

7.6 Operations and continuity.

- Agree maintenance windows and (if purchased) on-call arrangements.
- Participate in incident communications and post-incident reviews as requested.
- Attend training/knowledge-transfer sessions to support self-sufficiency.

7.7 Costs and charging.

- Pay cloud/platform and third-party usage charges directly, or reimburse pass-through costs where agreed.

7.8 Communications.

- Use the agreed support channels: email and ticketing (web chat and AI chat-bot tooling are not included in this listing; they may be commissioned separately under a Call-Off/SoW if required).
- Indicate any accessibility requirements for maintenance/incident notices.

---

8. Security, Information Assurance and Business Continuity

8.1 Approach and standards.
The Supplier operates security and service management controls aligned to NCSC Cloud Security Principles, UK GDPR/Data Protection Act 2018, and ISO-style governance (policy, risk, assurance, continual improvement). Controls are tailored to the Buyer environment and confirmed at Call-Off.

8.2 Roles and responsibilities.
Unless otherwise agreed, the Buyer is Controller and the Supplier is Processor for personal data processed under this Call-Off. The Buyer provides lawful basis, DPIAs (where required) and retention rules; the Supplier implements agreed technical/organisational measures and assists with requests, audits and incident handling.

8.3 Identity and access management (IAM).

- Least privilege and separation of duties.
- Named accounts; MFA enforced for privileged roles; break-glass with time-bound approval.
- Joiner–Mover–Leaver process and quarterly access reviews.
- Federated access to cloud consoles where supported; no shared credentials.
- Secrets management using cloud KMS/secret stores; no secrets in code/IaC.

8.4 Data protection and privacy.

- Encryption in transit (TLS 1.2+) and at rest using managed keys or KMS.
- Data location and residency controlled per Buyer policy; UK/EU regions by default unless otherwise agreed.
- Backups/snapshots follow Buyer retention rules with periodic restore testing.
- Sub-processing only with Buyer approval; a current sub-processor list is maintained.

8.5 Logging, monitoring and detection.

- Platform and application telemetry via CloudWatch/CloudTrail (or Buyer-selected equivalents) with standard retention.
- Centralised logs for admin actions, auth events and changes; integrity protection where supported.
- Alerting with P1–P3 routing and suppression during planned changes.

8.6 Vulnerability and change management.

- Regular vulnerability assessment of managed components; critical findings triaged and remediated to agreed timelines.
- All infrastructure changes via Infrastructure-as-Code with version control and peer review; change windows, rollback plans and post-change validation (smoke tests/dashboards).
- Optional secure code scanning for Buyer repositories where in scope.

8.7 Incident management and breach notification.

- Incidents are triaged to P1–P3 with restore targets per Section 5 (SLAs).
- Security incidents/personal data breaches are notified to the Buyer without undue delay and, where feasible, within 48 hours of confirmed awareness, with follow-up reporting on root cause, impact, containment and remediation.

8.8 Business continuity (BC) and disaster recovery (DR).

- RTO/RPO targets defined per service at Call-Off and validated through test restores.
- High-availability options (e.g., multi-AZ, autoscaling, managed databases) and resilience patterns (queue buffering, circuit breakers) used where required.
- DR exercises: at least annually for Gold, annually or as agreed for Silver/Bronze; results and actions recorded.

8.9 Maintenance, patching and supplier advisories.

- Planned maintenance with ≥48 hours' notice; urgent security maintenance aims for 24 hours' notice where risk allows; emergency maintenance follows incident comms (see Section 5.6).
- OS/runtime and managed service patching aligned to Buyer risk appetite and vendor advisories.

8.10 Assurance and audit.

- Evidence packs available on request (runbooks, network/IAM diagrams, logging/backup configurations, test results, change records).
- The Supplier will support reasonable Buyer audits/assurance activities and provide cooperation for regulatory requests related to the services.

8.11 Training and awareness.

- Project teams receive role-based security guidance; privacy-by-design and secure change practices are embedded in delivery.
- Buyer training/knowledge transfer provided per the Training section (runbooks, access patterns, cost controls, incident playbooks).

8.12 Exit security.
On termination/expiry, security tasks in the Exit Plan include data export/verification, revocation of access/keys, rotation of shared secrets/integrations, return or secure deletion of Buyer Data (per Buyer instruction and statutory retention), with evidence provided. (See Section 20 – Exit and Off-boarding.)

8.13 Dependencies and Buyer responsibilities.
Security outcomes depend on timely Buyer approvals, licensing for third-party tools (if any), and access to in-scope environments. Third-party or Buyer-managed components follow their owners' patch and incident processes; these dependencies will be reflected in the joint risk register and SLAs.

8.14 Statement of alignment.
Outage and maintenance management (notice periods, deployment safety patterns and recovery testing) operates per these T&Cs and Schedule 2 Service Levels, and is consistent with the Service Definition.

9. Data Protection (Controller/Processor)

9.1 Role. Parties' roles (Controller/Processor/Joint Controllers) are defined in the Order Form and Data Processing Schedule (Schedule 3).
9.2 Processing. Where the Supplier acts as Processor, it shall: (a) process Personal Data only on documented instructions; (b) ensure confidentiality; (c) implement appropriate technical and organisational measures; (d) assist with data subject rights, incident response and DPIAs; (e) use Sub-processors only with general or specific authorisation and on terms no less protective; (f) on termination, delete or return Personal Data as directed unless retention is required by law; and (g) make available information to demonstrate compliance and allow audit in accordance with Section 16.
9.3 International transfers will follow the Buyer's instructions and applicable safeguards (e.g., IDTA/UK Addendum to EU SCCs).
9.4 The Buyer shall ensure it has a valid lawful basis and provides required notices for the processing.

10. Change Control

10.1 Either party may propose a change via a change request describing scope, impact on Charges/timelines, and risk.
10.2 No change is binding until agreed in writing (including via the CCS portal).
10.3 Emergency changes for security, resilience or legal compliance may be implemented promptly, with notification to the Buyer.

11. Intellectual Property Rights

11.1 Background IPR remains with the originating party.
11.2 Deliverables: Unless otherwise stated in the Order Form, the Supplier grants the Buyer a perpetual, worldwide, royalty-free licence to use, copy and modify Deliverables for the Buyer's internal purposes and for the provision of public services.
11.3 Open-source software will be used under its applicable licences.
11.4 Third-party materials are licensed as stated by the third party.

12. Warranties

12.1 The Supplier warrants that it will perform the Services with reasonable skill and care in accordance with industry good practice.
12.2 Except as expressly stated, all other warranties are excluded to the fullest extent permitted by law.
12.3 The Supplier does not warrant that Services will be uninterrupted or error-free, particularly where reliant on Buyer or third-party platforms.

13. Liability and Insurance

13.1 Neither party excludes liability for death or personal injury caused by negligence, fraud, or any other liability which cannot be excluded by law.
13.2 Subject to 13.1, neither party shall be liable for: loss of profit, revenue, goodwill, or indirect/consequential losses.

13.3 Subject to 13.1–13.2, each party's total aggregate liability under the Agreement shall not exceed 100% of the Charges paid/payable in the 12 months preceding the claim (or, if the Agreement has run for less time, the amount payable for that period), unless otherwise required by the Call-Off terms.
13.4 The Supplier maintains the following insurance cover for the duration of the Services: (a) Employer's Liability £10,000,000; (b) Public Liability; (c) Professional Indemnity, each at levels appropriate to the Services. Certificates of insurance are available on request.

14. Subcontracting and Personnel

14.1 The Supplier may use vetted subcontractors and SMEs to deliver elements of the Services, remaining responsible for their performance.
14.2 Where required, named individuals and/or security clearances will be agreed in the Order Form.
14.3 The Supplier is an equal opportunities employer and operates inclusive and fair engagement practices.

15. Ethics and Compliance

15.1 The Supplier complies with applicable laws and policies on anti-bribery and corruption, modern slavery, tax evasion facilitation, equalities, accessibility, and sustainability.
15.2 The Buyer may request reasonable evidence of compliance, including policy statements and training records.
15.3 The Supplier will support the Buyer's social value objectives as set out in the Order Form and the Service Definition, and will provide reasonable evidence of related activities and outcomes in the monthly service report

16. Records, Audit and Transparency

16.1 The Supplier will maintain accurate records of Services and Charges for a minimum of seven (7) years.

16.2 Subject to reasonable notice and confidentiality, the Buyer and authorised auditors may audit relevant records and premises during business hours in line with framework rules.
16.3 The Supplier will reasonably assist with Freedom of Information Act requests as directed by the Buyer.

17. Confidentiality and Publicity

17.1 Each party shall protect the other's confidential Information and use it solely for the purposes of the Agreement.
17.2 Press releases or public statements about the Services require the other party's prior written consent, save where disclosure is required by law or the framework.

18. Environmental and Accessibility Commitments

18.1 The Supplier operates a remote-first and cloud-native approach to reduce emissions and will support Buyer Net Zero objectives where practicable.
18.2 The Supplier aims to meet relevant accessibility standards for deliverables and will follow Buyer guidance and standards.

19. Suspension and Termination

19.1 Precedence. These provisions apply in addition to, and shall be interpreted consistently with, the CCS G-Cloud 15 Framework Agreement (RM6350) and the applicable Call-Off Contract (including its Schedules). Where there is any conflict, the Framework Agreement and the applicable Call-Off Contract take precedence.

19.2 Termination for breach. Either party may terminate where the other commits a material breach which (a) is capable of remedy and is not remedied within 30 days of written notice (or such other cure period as stated in the Call-Off), or (b) is irremediable. Repeated or persistent material breaches may be treated as a material breach.

19.3 Termination for insolvency/mandatory grounds. Either party may terminate immediately on written notice where the other becomes insolvent, or where termination is required by law, regulation, government policy, or the applicable Call-Off terms.

19.4 Buyer termination for convenience. Notwithstanding any other provision, the Buyer may terminate the Call-Off Contract (in whole or in part) for convenience on 30 days' written notice at any time, in accordance with the CCS G-Cloud Framework and Call-Off terms. No early termination charges apply beyond payment for Services duly performed up to the effective termination date.

19.5 Suspension for non-payment. The Supplier may suspend Services for undisputed overdue Charges following 10 Working Days' prior written notice, unless prohibited by the Call-Off terms. Suspension shall cease promptly upon receipt of the overdue amount. No suspension shall prevent the Supplier from complying with any Exit and Off-boarding obligations.

19.6 Mutual termination. The parties may terminate by written agreement at any time.

19.7 Effect of termination. Termination or expiry is without prejudice to accrued rights and obligations. The Buyer shall pay for Services properly performed up to the effective date of termination/expiry, subject to any set-off or withholding permitted or required under the Call-Off or applicable law. Data return, deletion and transition assistance are provided in accordance with Section 20 (Exit and Off-boarding).

19.8 Survival. Clauses relating to confidentiality, intellectual property, data protection, records/audit, limitation of liability, charges and payment (to the extent accrued), and Section 20 (Exit and Off-boarding) survive termination or expiry.

---

20. Exit, Off-Boarding and Data Return/Deletion

20.1 Purpose and trigger.
On expiry or termination of the Call-Off (for any reason), the Supplier will provide structured exit assistance to ensure continuity of service, protection of Buyer Data and a clean, auditable handover to the Buyer and/or an incoming supplier.

20.2 Standard exit assistance (included).
Within the notice period stated in the Order Form, the Supplier will deliver an Exit Plan and the following activities:

- **Exit plan & checklist** covering scope, roles (RACI), timelines, acceptance criteria and risks/mitigations.

- **Knowledge transfer**: runbooks, operating procedures, CI/CD and change workflows, access model, backup/restore and DR approach.
- **Artefact & configuration export**: source code and Infrastructure-as-Code repositories (where in scope), build artefacts, deployment manifests, environment variables (redacted/secrets via secure store), logging/metrics dashboards and alert rules.
- **Data export** in Buyer-agreed open formats (e.g., CSV/JSON/Parquet, snapshots, exports or backups), plus schema and integrity checks.
- **Access re-scoping**: rotation/revocation of secrets, keys, roles and service accounts; removal of Supplier identities; hand-back of ownership for cloud accounts/resources where applicable.
- **Handover session** with the Buyer/incoming supplier and documented sign-off.

20.3 Enhanced off-boarding / migration (optional).
If requested by the Buyer, the Supplier can provide additional transition services, including:

- **Exit Readiness Assessment** (environment/data flow inventory, dependency/risk review).
- **Parallel environment build** (landing zone, IaC baselines, CI/CD bootstrapping).
- **Data migration & validation** (mapping, secure transfer, reconciliation, rollback).
- **Re-host/re-platform support** (containerisation, policy/identity/secret porting, integration re-wiring).
- **Cutover management** (rehearsals, change window, DNS/traffic switch, hypercare).
- **Decommissioning & clean-up** (safe teardown, retention/disposal, cost/permission hygiene).
  These services are delivered on a Time-and-Materials basis at published day rates (see Schedule 1 – Optional Services: Off-boarding & Transition) and are planned and approved via a transition work order.

20.4 Timelines (typical).

- **Exit Plan** issued within 5 working days of termination/expiry notice (or as otherwise agreed).
- **Data/artefact export** completed within the notice period and verified as readable/usable by the Buyer/incoming supplier.
- **Handover session** held before service end date.
- **Hypercare** (if purchased) runs for the agreed period after cutover.

20.5 Acceptance criteria.
Exit is complete when: (a) the named artefacts and data have been exported and verified; (b) Supplier access has been revoked/rotated with evidence; (c) a handover session has been delivered; and (d) any agreed hypercare period has concluded.

20.6 Data return and deletion.

- **Return:** Buyer Data will be returned in the agreed open formats and by secure transfer mechanism.
- **Deletion:** Following Buyer confirmation that return is complete, the Supplier will securely delete remaining copies of Buyer Data under Supplier control (excluding backups subject to statutory/contractual retention) and provide a deletion certificate within 10 working days.
- **Backups/retention:** Any residual backups containing Buyer Data are retained only for the period required by law or regulation, then securely deleted according to Supplier policy; such retention will be disclosed in the Exit Plan.

20.7 Roles, responsibilities and cooperation.

- The Buyer will provide timely approvals, access and decision-maker availability, and will arrange participation by any incoming supplier.
- The Supplier will cooperate reasonably with Buyer-nominated third parties and maintain a joint RAID log during the exit period.

20.8 Licensing, IP and tools.

- Buyer IP, configurations and data are returned as above. Any Supplier proprietary tools/accelerators are excluded unless licensed separately; their outputs (runbooks, config, IaC written for the Buyer) are included.
- Third-party licences (e.g., observability tools) remain subject to their own terms; the Exit Plan will identify any Buyer actions required to novate or replace them.

20.9 Security during exit.
Exit activities follow least-privilege access, change control and audit logging. Access reductions are sequenced to avoid service impact and are fully evidenced. Security/BC controls remain in force until exit completion (see Sections 5 and 8).

20.10 Charges.

- Standard exit assistance in 20.2 is included in the service.
- Optional services in 20.3 are chargeable on Time-and-Materials at published day rates (Schedule 1). Out-of-hours work uses the Rate Card uplift.

20.11 Survival.
Confidentiality, data protection, liability, IP and audit obligations survive termination to the extent required by law or expressly stated in these T&Cs and the Order Form.

20.12 No service interruption.
The Supplier will not unreasonably withhold or delay cooperation during exit and will take reasonable steps to avoid service interruption during the agreed transition period.

21. Force Majeure

Neither party is liable for delay or failure to perform due to events beyond reasonable control. The affected party will notify the other and use reasonable efforts to mitigate.

22. Dispute Resolution

Parties will seek to resolve disputes through escalation to senior representatives. If unresolved, the dispute shall be handled per the Call-Off dispute resolution provisions and, failing that, the courts of England and Wales.

23. Notices

Formal notices shall be sent to the contacts stated in the Order Form by email and one of recorded post or courier, and deemed received in accordance with the Call-Off terms.

24. Assignment

Neither party may assign or transfer its rights or obligations without the other’s prior written consent, except as permitted by the framework.

25. Entire Agreement and Variation

These Supplemental Terms, together with the Call-Off, constitute the entire agreement relating to their subject matter. Variations must be in writing and signed (including via CCS portal mechanisms).

26. Governing Law

This Agreement is governed by and construed in accordance with the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales, subject to any framework-mandated provisions.

Schedules

Schedule 1 – Rates and Commercials

1) Pricing principles

- **Rate basis:** Time & Materials using the Supplier's **published G-Cloud Rate Card** referenced in the Order Form.
- **UoM:** 1 day = 7.5 hours (half-day/hourly by agreement).
- **Scope alignment:** Chosen **support level (Bronze/Silver/Gold)** and Buyer criticality determine role mix/effort.
- **Exclusions:** Hyperscaler/SaaS and third-party costs are Buyer's responsibility (pass-through if agreed).
- **Service Credits:** As per **Section 5** (exclusive remedy).

2) Roles and day rates

- Roles (e.g., **Cloud Support/DevOps Engineer**, **Cloud Architect/Technical Lead**, **Technical Account Manager**, **Delivery Manager**, **Data/Platform Engineer**) are charged at **published Rate Card** day rates.
- The Order Form states the applicable rates and any minimum monthly commitment.

3) Support levels – commitments (summary)

- **Bronze / Silver / Gold** coverage as described in the **Service Definition** and **Schedule 2**; actual monthly commitments are **finalised at Call-Off** (and may include on-call where agreed).

4) Optional services – Off-boarding & Transition

- Available on **Time & Materials** at Rate Card rates (e.g., Exit Readiness Assessment, Handover Sprint, Managed Transition, Decommissioning, Hypercare).
- Scope and effort confirmed at Call-Off; see Service Definition – Off-Boarding.

5) Out-of-hours & on-call

- Provided by agreement at the **Rate Card uplift**. **Where on-call is purchased, applicable response targets and restore expectations are confirmed at Call-Off and reflected in the monthly service report.**

6) Travel & expenses

- **Remote-first** delivery; on-site only by Buyer request/approval and recharged at cost per Order Form.

7) Invoicing & payment

- **Monthly in arrears** for T&M; any fixed **minimum monthly** charges in advance.
- Payment terms per Order Form.
- Any Service Credits are netted from the next invoice (or refunded by agreement).

8) Changes

- Changes to scope/support level via change control; priced at Rate Card rates. Buyer may vary minimum commitment or support level on **30 days' notice**, subject to capacity.

Schedule 2 – Service Levels

Support hours

- 09:00–18:00 UK, Monday–Friday (on-call by agreement).

Support channels

- **Email and ticketing** (no web chat under this listing).

Severity (guide)

- P1 Critical: full outage/major impact, no workaround.
- P2 High: significant impact, workaround exists.
- P3 Normal: minor impact / routine request.

Response targets (by support level)

- Bronze: P1 1h | P2 4h | P3 1 business day
- Silver: P1 30m | P2 2h | P3 8h
- Gold: P1 15m | P2 1h | P3 4h

Availability targets (managed environments)

- Bronze: 99.5% | Silver: 99.9% | Gold: 99.95% (monthly)

Maintenance notice

- Planned: ≥ 48 hours; out-of-hours where possible.
- Urgent security: aim 24 hours where risk allows.
- Emergency: immediate with incident-style updates.

Service desk KPI

- ≥ 95% of tickets receive a first human response within the applicable SLA each month.

Measurement & exclusions

- Availability measured at the service/application boundary we operate, over the monthly billing period.
- Excludes agreed maintenance windows and exclusions set out in Section 5 (T&Cs).

Reporting & reviews

- Monthly service report (incidents, availability, requests, optimisation actions).
- Post-incident review within 5 working days for P1 (and major P2).

Escalation

- Named Technical Lead and Delivery/Account contact; Buyer to provide corresponding escalation contacts.

Notes

- SLAs/targets are finalised at Call-Off based on scope, criticality, upstream provider SLAs and any on-call requirement.
- Financial remedies (Service Credits) as set out in Section 5 – Service Levels and Service Credits.

Schedule 3 – Data Processing Schedule (DPA)

1. **Subject Matter and Duration:** provision of the Services for the Term.
2. **Nature and Purpose:** hosting/support, integration, migration, monitoring, analytics enablement.
3. **Types of Personal Data:** as specified by the Buyer (may include contact data, usage logs, and service records).
4. **Categories of Data Subjects:** Buyer employees, contractors, citizens/end-users as relevant.
5. **Processing Activities:** storage, access, transmission, analysis for support, logging and monitoring.
6. **Security Measures:** access control, encryption in transit/at rest, network segregation, vulnerability management, logging/audit, backup and recovery, secure SDLC/CI-CD.
7. **Sub-processors:** The Supplier may engage UK/EU-based cloud providers and specialist SMEs. A current sub-processor list is available on request and will be provided prior to onboarding.
8. **International Transfers:** only with Buyer approval and appropriate safeguards (IDTA/UK Addendum to EU SCCs).
9. **Breach Notification:** without undue delay and within agreed timeframes, providing required details and cooperation.
10. **Deletion/Return:** on Buyer instruction at exit, subject to statutory retention.

Schedule 4 – Security and Compliance Commitments (Summary)

- **Standards alignment:** NCSC guidance; ISO-aligned information security controls.
- **Access management:** least privilege, MFA, role-based IAM.
- **Environment segregation:** dev/test/stage/prod with change approvals.

- **Monitoring & logging:** cloud-native and third-party tools; retention per Buyer policy.
- **Vulnerability & patching:** regular reviews and remediation by risk.
- **Business continuity:** remote-first operations; restoration objectives agreed per system.
- **Personnel:** appropriate screening; clearances as required by the Order Form.
- **Policies:** anti-bribery, modern slavery, equality, environmental and wellbeing policies maintained; evidence available on request.

Schedule 5 – Deliverables & Acceptance

- Deliverables listed in the Order Form (e.g., architecture docs, IaC, runbooks, dashboards).
- Acceptance criteria and timelines per Section 6.

Schedule 6 – Exit Plan (Outline)

- Knowledge transfer sessions and documentation handover.
- Credentials and secrets rotation; access revocation plan.
- Data export and verification steps; backup snapshots where appropriate.
- Handover to Buyer or replacement supplier; outstanding risks and actions log.
- Post-exit support window (if requested) on time-and-materials basis.

Signatures (for reference if required outside Jaggaer/CCS portal)

Buyer: _____
Name/Title: _____
Date: _____

Supplier (CHRIS JOHNSON Studio LTD): _____
Name/Title: _____
Date: _____