cXc Platform Terms — Schedules 1 and 2

Version 1.1 · effective [date] · published at mycxc.services/terms

These Schedules are incorporated into the Master Sales and Services Agreement between conXchange Pvt Ltd and the Customer by clause 2.4 of that Agreement, and are amended only in accordance with it. Prior versions are retained and available on request.

SCHEDULE 1 — SUPPORT, SERVICE LEVELS AND RESILIENCE

1. Support. Support is provided to trained Authorised Users during Business Hours via the support portal and email (support@mycxc.services), with telephone follow-up for Severity 1 and 2 incidents. The Customer shall channel requests through no more than two nominated support contacts who triage internal queries first. Support is conditional on the Customer being current in payment, requests being logged with reproduction steps, error messages and impact, and the requesting user having completed onboarding training; the Supplier may decline or charge for support otherwise.

2. Severity levels and response targets. Response targets are measured within Business Hours from logging of a properly detailed ticket; severity is assigned by the Supplier acting reasonably, taking the Customer's classification into account; resolution times are targets, not guarantees.

Severity	Definition	Target response / update
Severity 1	Production Platform unavailable or unusable for all users; no workaround	Response within 1 Business Hour; updates every 2 Business Hours; continuous effort during Business Hours until resolved or workaround
Severity 2	Business-critical function failing for key users; no reasonable workaround	Response within 2 Business Hours; updates every 4 Business Hours
Severity 3	Non-critical function impaired; workaround available	Response within 8 Business Hours; resolution targeted in ordinary release cycle
Severity 4	Questions, cosmetic issues, enhancement requests	Response within 2 Business Days; enhancements at Supplier's roadmap discretion

3. Availability and service credits. The Supplier targets Platform availability of 99.5% per calendar month, measured by its monitoring systems, excluding planned maintenance notified in advance, emergency maintenance, Relief Events, Third-Party Services, internet and telecommunications failures, the Customer's systems, connectivity and configurations, Free/Beta Services, and suspension under clause 9. The Supplier shall use reasonable endeavours to schedule planned maintenance outside Business Hours and to give at least 5 Business Days' notice of it. Availability information for the preceding month is available on request. If availability falls below 99.5%, the Customer may claim within 30 days of month end a service credit of 5% of that month's attributable Subscription Fees, rising to 10% below 98.0%. Credits apply against future invoices only; require the Customer to be current in payment of undisputed Fees; are capped at 10% of monthly-equivalent Subscription Fees in any month and 5% of annual Subscription Fees in any contract year; are not payable in cash and are forfeited on termination; and are the sole and exclusive remedy for availability and Service Level failures.

4. Exclusions. Support does not include: support of the Customer's own systems, networks, browsers or third-party software; data cleansing or re-keying; consultancy, configuration or training (chargeable as additional services agreed in writing); investigation of issues caused by Customer misuse, unsupported configurations or Relief Events (chargeable at time-and-materials rates where investigated at the Customer's request); or bespoke report writing.

5. Resilience, continuity and disaster recovery. The Supplier maintains business continuity and disaster recovery arrangements appropriate to the Services, including the backup, restoration and recovery objectives in Schedule 2 (recovery point objective 24 hours, recovery time objective 48 hours — objectives, not guarantees), with backup and restoration testing at least annually. The Supplier shall notify the Customer without undue delay of any incident or change it reasonably expects to have a material adverse effect on the resilience or continuity of the Services, and

shall provide reasonable cooperation and information to support the Customer's operational resilience and outsourcing obligations, including its outsourcing register and impact-tolerance mapping. Such cooperation is limited to information in the Supplier's possession relating to the Services, may be provided through its independent assurance reports where available, and may be charged at then-current rates beyond a reasonable standard level of effort. No recovery outcome or timeframe is guaranteed beyond the stated objectives, and the Customer has no operational step-in right in respect of the Supplier's systems or operations.

SCHEDULE 2 — DATA PROTECTION AND INFORMATION SECURITY

Part 1 — Processing terms (Article 28 UK GDPR)

1.1 Roles and scope. For Personal Data comprised in Customer Data, the Customer is controller and the Supplier is processor. Subject-matter: provision of the Services. Duration: the Term plus the retention period in Part 3. Nature and purpose: hosting, storage, workflow processing, screening orchestration, display, transmission, backup and support. Data subjects: Counterparty Representatives, Authorised Users and other individuals whose data the Customer records. Categories: identity, contact, professional, licensing and appointment data; due diligence and screening results, which may include criminal offence and special category data where the Customer configures such checks; and correspondence. The Customer is responsible for an appropriate lawful basis and, where applicable, an Article 10 or DPA 2018 condition for all such data.

1.2 Processor obligations. The Supplier shall: (a) process Personal Data only on the Customer's documented instructions, comprising this Agreement and the Customer's configuration and use of the Platform, unless required otherwise by law, in which case it will inform the Customer unless prohibited; (b) ensure persons authorised to process are bound by confidentiality; (c) implement the measures in Part 2; (d) assist the Customer, at the Customer's reasonable cost, with data subject requests and its obligations under Articles 32 to 36 UK GDPR, taking into account the nature of the processing; (e) notify the Customer without undue delay, and in any event within 48 hours, of becoming aware of a confirmed Personal Data Breach affecting Customer Data, providing the information reasonably available to it, in phases if necessary, and cooperating reasonably with the Customer's investigation, containment, remediation, regulator notifications and data-subject communications; (f) at the Customer's election, delete or return Personal Data at the end of the Services under clause 9.4 and Part 3; and (g) make available information reasonably necessary to demonstrate compliance and allow audits strictly under clause 17.2, which the parties agree satisfies Article 28(3)(h).

1.3 Instructions and indemnity. The Supplier may charge, at time-and-materials rates, for assistance or instruction-compliance beyond the standard functionality of the Platform. The Customer shall indemnify the Supplier against Losses arising from processing performed in accordance with the Customer's documented instructions or configurations, including any claim that an instruction infringes Data Protection Legislation (the Supplier shall inform the Customer if it forms that view, without an obligation to review instructions).

1.4 Sub-processors. The Customer grants general written authorisation for the Supplier's engagement of sub-processors, being third parties engaged to process Personal Data comprised in Customer Data, including hosting, infrastructure, screening and e-signature providers. The categories engaged at the date of this Agreement are listed in the Sub-processor Annex. The Supplier shall: (a) impose data protection obligations materially equivalent to this Schedule on each sub-processor; (b) remain responsible for its performance; and (c) give at least 30 days' prior notice of any material addition or replacement, which the Customer may elect to receive via the Supplier's trust page.

1.5 Objections. The Customer may object to a material new sub-processor on documented, reasonable data-protection grounds within the notice period. On a valid objection the parties shall discuss in good faith and the Supplier shall use reasonable endeavours to offer a commercially reasonable configuration change or workaround avoiding that sub-processor. If none is reasonably available, the Supplier may suspend the affected feature, or the Customer may as its sole and exclusive remedy terminate the affected processing or Order Form on notice, with a pro-rata refund of prepaid unused Subscription Fees for that Order Form only, excluding additional services, Pass-Through Charges and expenses. Objection confers no general veto over the Supplier's choice of sub-processors or hosting.

1.6 Location and transfers. Primary hosting and backup of Customer Data is in data centres within the European Union or such other region as the Order Form states. The Supplier shall not transfer Customer Data containing Personal Data outside the United Kingdom or the European Economic Area unless the transfer is to a country benefiting from UK adequacy regulations or is subject to appropriate safeguards under Articles 44 to 49 UK GDPR, including the UK IDTA or Addendum, and support access from other locations is protected accordingly. The Supplier shall notify the Customer before any material change to the hosting geography and shall ensure appropriate safeguards for any transfer to a non-adequate country.

Part 2 — Information security

2.1 Baseline. The Supplier maintains an information security programme with technical and organisational measures aligned to the principles of ISO/IEC 27001 and the SOC 2 trust services criteria, proportionate to the data processed, including: encryption of Customer Data in transit (TLS 1.2+) and at rest; logical segregation of customer environments; role-based access control, least privilege and MFA for administrative access; vulnerability management and patching; secure development lifecycle; logging and monitoring; personnel vetting and security

training; and supplier security assessment. Formal certification is not a contractual obligation unless expressly agreed in an Order Form.

2.2 Backups and disaster recovery. Production Customer Data is backed up at least daily, with backups retained on a rolling cycle of at least 30 days and stored within the hosting region. The Supplier maintains and periodically tests a disaster recovery plan targeting a recovery point objective of 24 hours and a recovery time objective of 48 hours, as objectives rather than guarantees. The Customer remains responsible for its own business continuity and for retaining source data under clause 11.4.

2.3 Incident notification. The Supplier shall notify the Customer without undue delay of any confirmed material security incident affecting the confidentiality, integrity or availability of the Services or Customer Data, and for a confirmed Personal Data Breach within the period in paragraph 1.2(e), and shall cooperate reasonably with containment, investigation, remediation and any notifications the Customer must make. Notification is not an admission of fault; the Supplier's responsibility is limited to failures of its own security obligations under this Schedule, and it does not guarantee that no incident will occur.

Part 3 — Retention and deletion

3.1 Following termination of this Agreement (or the affected Order Form), the Supplier shall delete or irreversibly anonymise Customer Data from production systems within 90 days of the later of that termination and the end of any Exit Period under clause 9.5, and from backups through the ordinary backup rotation cycle (not exceeding a further 90 days), subject to the retention rights in clause 9.4. On written request, the Supplier will confirm deletion in writing.

Sub-processor Annex

Category	Function	Location (indicative)
Cloud hosting & infrastructure	Hosting, storage, compute and backup of Customer Data	European Union
Screening (sanctions / PEP / adverse media / background)	Counterparty and Counterparty Representative screening	United Kingdom / European Union
Licensing & appointment registries	Licence and appointment verification data	United Kingdom / European Union
Credit reference	Counterparty credit checks	United Kingdom
E-signature	Execution of agreements and documents	United Kingdom / European Union

Named sub-processors within each category are set out on the Supplier's trust page and provided on request; this Annex may be updated by notice under paragraph 1.4.