Terms of Service Agreement

Effective Date: July 10th, 2026

This **Terms of Service Agreement** ("Agreement") is a legally binding contract between **Nuworks Ltd**, a company incorporated and registered in England, trading as **BrokerCentral** ("BrokerCentral", "Provider", "we", "our", or "us"), and the individual or entity ("Customer", "you", or "your") that accesses, installs, or uses the BrokerCentral software and related services (the "Services").

The BrokerCentral Services are offered to the Customer subject to its acceptance of these BrokerCentral Terms of Service (the "Terms"). By accessing, installing, or using the BrokerCentral Services, or by otherwise indicating assent to these Terms, the Customer enters into a legally binding contract with BrokerCentral.

IF YOU ARE ENTERING INTO THESE TERMS ON BEHALF OF AN ENTITY, SUCH AS YOUR EMPLOYER OR THE COMPANY YOU WORK FOR, YOU REPRESENT AND WARRANT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND SUCH ENTITY. IN SUCH A CASE, THE TERMS "YOU," "YOUR," "CUSTOMER," OR ANY SIMILAR CAPITALISED TERM HEREIN WILL REFER TO SUCH ENTITY.

These Terms constitute a contract governing the Customer's use of the BrokerCentral Services and include the following documents expressly incorporated by reference:

- the applicable Order Form;
- the Acceptable Use Policy (AUP);
- the Data Processing Agreement (DPA); and
- any additional schedules, supplemental terms, service-specific terms, or documents expressly incorporated by reference in the applicable Order Form or these Terms.

BY REGISTERING FOR, PURCHASING ACCESS TO, ACCESSING, AND/OR USING THE BROKERCENTRAL SERVICES OR OTHERWISE INDICATING ASSENT, YOU REPRESENT AND WARRANT THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO BE BOUND BY THESE TERMS. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS, DO NOT ACCESS OR USE THE BROKERCENTRAL SERVICES.

ANY DISPUTE ARISING OUT OF OR IN CONNECTION WITH THESE TERMS OR THE BROKERCENTRAL SERVICES SHALL BE HANDLED IN ACCORDANCE WITH THE DISPUTE RESOLUTION PROVISIONS SET OUT IN SECTION 17 BELOW AND THE GOVERNING LAW AND JURISDICTION PROVISIONS SET OUT IN SECTION 18.6 BELOW.

THE PARTIES WILL FIRST SEEK TO RESOLVE DISPUTES THROUGH GOOD FAITH NEGOTIATIONS BETWEEN AUTHORISED REPRESENTATIVES. IF A DISPUTE CANNOT BE RESOLVED THROUGH THOSE NEGOTIATIONS, THE COURTS OF ENGLAND AND WALES SHALL HAVE EXCLUSIVE JURISDICTION, SUBJECT TO ANY RIGHTS TO SEEK INTERIM, INJUNCTIVE, EQUITABLE, DEBT RECOVERY, OR INTELLECTUAL PROPERTY-RELATED RELIEF WHERE PERMITTED UNDER THESE TERMS.

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement

- “Affiliate” means, in relation to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party, where “control” means ownership of more than fifty percent (50%) of the voting rights or equity interests of the relevant entity.
- “Agreement” means this Software-as-a-Service agreement (including its Schedules) and any amendments made to it from time to time.
- “Add-On Feature” means a feature or set of features within the Platform that are subject to additional charges, as set forth in the Order Form and/or during the purchase process, and may be subject to additional terms as outlined in the Order Form.
- “AI Functionality” means any aspects of the Platform that are powered by artificial intelligence, machine learning, or similar technologies.
- “Authorised User” means an individual employee authorised by the Customer to access and use the Platform under the Customer’s account in accordance with this Agreement, the applicable Order Form, and the Customer’s permitted Subscription entitlements.
- “Business Day” means any weekday other than a bank or public holiday in the United Kingdom.
- “Business Hours” means the hours between 09:00 and 17:00 on a Business Day.
- “Charges” means one-time, additional, or variable payments for services outside the standard Subscription, including but not limited to: payments for Additional Projects; charges for bespoke modifications or requested enhancements; late payment penalties; one-time costs for exceeding usage limits beyond the agreed Subscription plan.
- “Customer Confidential Information” means:
    - (a) any information disclosed (whether in writing, orally, or otherwise) by the Customer to the Provider that is marked as “confidential”, described as “confidential”, or should have been understood by the Provider at the time of disclosure to be confidential;
    - (b) the financial terms and conditions of this Agreement;
    - (c) the Customer Materials; and
    - (d) any other information that a reasonable person or entity would consider confidential in nature.
- “Customer Data” means any data, information, content, records, files, Personal Data, or other materials submitted to, stored on, processed by, or transmitted through the Platform by or on behalf of the Customer, including Customer Materials.
- “Customer Materials” means all data, works, and materials:
    - (a) uploaded to, stored on, processed using, or transmitted via the Platform by or on behalf of the Customer, or by any person, application, or automated system using the Customer's account; and
    - (b) otherwise provided by the Customer to the Provider for the purposes of or in connection with this Agreement.
- “Data Protection Laws” means all applicable laws, regulations, regulatory requirements, statutory guidance, and codes of practice relating to Personal Data, privacy, electronic communications, direct marketing, cookies, similar tracking technologies, or AI-enabled processing, in each case to the extent applicable to Personal Data, privacy, electronic communications, or AI-enabled processing, including:
- (a) the UK General Data Protection Regulation (“UK GDPR”);
- (b) the Data Protection Act 2018;
- (c) the Privacy and Electronic Communications Regulations 2003 (“PECR”);
- (d) the Data (Use and Access) Act 2025 (“DUAA 2025”);
- (e) any legislation by which the foregoing is amended, replaced, supplemented or re-enacted; and
- (f) any binding guidance, statutory codes, or regulatory requirements issued by the Information Commissioner’s Office (“ICO”) or other competent supervisory authority.
- “Defect” means a defect, error, or bug that has an adverse effect on the appearance, operation, or functionality of the Platform, but excluding any defect, error, or bug that arises from or is caused by:
    - (a) an act or omission of the Customer, or an act or omission of one of the Customer's employees, officers, agents, suppliers, or subcontractors; or
    - (b) an incompatibility between the Platform and any system, application, program, or software not specified as compatible in the Order Form.
- “Documentation” means the materials provided by the Provider to the Customer that specify how the Platform should be used.
- “Effective Date” means the date on which this Agreement is executed, as set out in the Order Form.
- “Fees” means recurring payments associated with the Customer’s Subscription to the Platform, including Standard Subscription Fees, Add-On Feature fees, Renewal Fees, Licence Fees, and recurring fees for additional users, usage capacity, upgraded entitlements, premium services, or other recurring services specified in the Order Form or otherwise agreed between the parties.
- “Intellectual Property Rights” means all intellectual property rights wherever in the world, whether registered or unregistered, including any application or right of application for such rights. This includes copyrights, related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semiconductor topography rights, and design rights.

- “Licence Fees” means Fees specifically related to the Customer’s right to access and use the Platform, as outlined in the Order Form. These may be subject to increases due to Add-On Features, Additional Projects, or modifications requested by the Customer.
- “Open-Source Software” means software licensed under an open-source license as defined by the Open Source Initiative or the Free Software Foundation.
- “Personal Data” means any information relating to an identified or identifiable natural person as defined under applicable Data Protection Laws.
- “Permitted Purpose” means the Customer's right to use the Platform for its internal business operations only.
- “Platform” means the software platform known as ‘BrokerCentral’ that is owned and operated by the Provider, and that will be made available to the Customer as a service via the internet under this Agreement.
- “Schedule” means any schedule attached to and incorporated into this Agreement.
- “Services” means all services provided or to be provided by the Provider to the Customer under this Agreement, including but not limited to the Support Services.
- “Subscription” means the period specified as such in the Order Form.
- “Supplemental Terms” means the additional terms, as set forth in the Order Form, applicable to the Customer’s use of certain features, services, or third-party integrations.
- “Support Services” means support and maintenance services provided or to be provided by the Provider to the Customer in accordance with Schedule 1.
- “Term” means the duration of this Agreement as set out in the Order Form.
- “Tracking Technologies” means cookies, pixels, SDKs, scripts, tags, analytics technologies, local storage objects, telemetry technologies, session technologies, and similar tracking or electronic communications technologies.
- “Upgrades” means new versions or updates to the Platform, whether for the purpose of bug fixes, security patches, or functional enhancements.

1.2 Statutory References

In this Agreement, a reference to a statute or statutory provision includes a reference to:

(a) that statute or statutory provision as amended, replaced, supplemented or re-enacted from time to time; and

(b) any subordinate legislation made under that statute or statutory provision.

1.3 Clause Headings

The Clause headings do not affect the interpretation of this Agreement.

1.4 Ejusdem Generis Rule

The ejusdem generis rule is not intended to be used in the interpretation of this Agreement.

2. TERM

2.1 Commencement and Duration

- This Agreement shall commence on the **Effective Date** and shall continue until the **Term Expiry Date** specified in the Order Form, unless terminated earlier in accordance with Clause 13.

2.2 Subscription and Fees

- To access and use the Platform and Services, the Customer must select a Subscription and pay the applicable Subscription Fees. The Subscription shall define the Customer’s permitted use of the Platform, including the number of authorised users, features, and service level entitlements, as detailed in the Order Form.

2.3 Additional Entitlements

- The Customer may purchase additional entitlements, including expanded user access or upgraded features, subject to payment of additional Fees. Any such upgrades shall be governed by the terms of this Agreement and shall run concurrently with the existing Subscription.

2.4 Automatic Renewal

Unless otherwise agreed in writing, this Agreement shall automatically renew for successive periods equal to the initial Subscription Term unless either party gives written notice of non-renewal at least:

(a) 60 days prior to the Term Expiry Date for Subscriptions with a term longer than one month; or

(b) 7 days prior to the Term Expiry Date for rolling monthly Subscriptions.

Each renewal shall be subject to the Fees, Subscription entitlements, service terms, and policies applicable immediately prior to renewal, subject to:

(a) any annual CPI-based Fee adjustment permitted under Clause 7.5;

(b) any pricing, usage, entitlement, or renewal changes expressly stated in the applicable Order Form;

(c) any additional Fees for Add-On Features, New Functionality, Additional Projects, increased usage, additional users, upgraded entitlements, support services, professional services, or premium services ordered, enabled, agreed to, or used by the Customer; and

(d) any changes to incorporated policies or service documents made in accordance with Clause 18.7.

The Provider shall give the Customer reasonable prior notice of any material change to Fees applicable on renewal, except where the change arises from an annual CPI-based adjustment under Clause 7.5, an existing Order Form mechanism, or additional Fees for services, functionality, usage, or entitlements ordered, enabled, agreed to, or used by the Customer.

If the Customer does not agree to a notified material change to Fees applicable on renewal, the Customer may elect not to renew the affected Services by giving notice in accordance with this Clause 2.4.

Continued access to or use of the Services following renewal constitutes acceptance of the renewed Fees and applicable terms.

3. THE PLATFORM

3.1 Access to the Platform

- The Provider will make the Platform available to the Customer by setting up an account and providing login credentials as soon as practicable following the Effective Date, provided the applicable Fees have been paid.

3.2 Licence to Use the Platform

- Subject to the limitations in Clause 3.3, the prohibitions in Clause 3.4, and the Provider's rights of suspension or termination under this Agreement, the Provider grants the Customer a non-exclusive, non-transferable licence during the Subscription Term to access and use the Platform for the Permitted Purpose in accordance with the Documentation.

3.3 User Access and Entitlements

- The licence granted under Clause 3.2 is subject to the following limitations:
    - User Restrictions – The Platform may only be used by the number of concurrent or named users specified in the Order Form. The Customer may request additional user access, subject to payment of additional Fees.
    - Authorised Users – The Platform may only be used by the employees of the Customer, except where third-party access is expressly agreed in the Order Form and in this Agreement.
    - Acceptable Use – The Customer and its users must comply at all times with the Acceptable Use Policy (AUP).

3.4 Prohibited Uses

Except where required by law or expressly permitted in this Agreement:

(a) The Customer may not sub-license, rent, or assign its right to use the Platform, except as provided in Clauses 3.8 and 3.9.

(b) The Customer must not frame, re-publish, or redistribute any part of the Platform.

(c) The Customer must not alter, adapt, reverse engineer, decompile, disassemble, or modify the Platform.

3.4.1 Compliance with Sanctions and Export Controls

The Customer must comply with all applicable sanctions, export control, trade compliance, and import laws relating to its access to and use of the Platform and Services. The Provider may suspend, restrict, or terminate access to the Services where reasonably necessary to comply with applicable sanctions, export control laws, trade restrictions, or regulatory requirements, or where continued provision of the Services may expose the Provider to legal, regulatory, or reputational risk.

3.5 Modifications to the Platform

The Provider may update, modify, enhance, replace, suspend, or discontinue parts of the Platform from time to time, including to improve functionality, maintain security, comply with applicable law, or reflect changes to the Services.

Where reasonably practicable, the Provider will provide advance notice of material changes that are likely to materially adversely affect the Customer's use of the Platform.

Nothing in this Clause prevents the Provider from making immediate changes where necessary for security, legal, operational, or technical reasons.

The Provider will use commercially reasonable efforts to avoid materially reducing the core functionality of the Platform during the applicable Subscription Term.

3.6 Intellectual Property Rights

- The Platform, including all Intellectual Property Rights, shall remain the exclusive property of the Provider. The Customer has no rights to the source code or object code unless explicitly agreed otherwise in a separate written agreement with the Provider.

3.7 Security and Account Responsibility

The Customer must:

(a) Use all reasonable endeavours to ensure that unauthorised persons do not access the Platform using the Customer's credentials.

(b) Notify the Provider immediately in case of unauthorised access, data breaches, or credential misuse.

(c) Be responsible for ensuring the security of user credentials and account access, including by implementing reasonable account security practices. The Customer is responsible for enabling available multi-factor authentication (MFA) where appropriate, particularly for administrative or privileged accounts. The Provider is not liable for breaches, unauthorised access, or credential misuse caused by weak, shared, compromised, or inadequately protected Customer credentials, or by the Customer's failure to implement reasonable account security controls.

The Provider shall:

(d) maintain appropriate technical and organisational measures designed to protect Customer Materials and Personal Data against unauthorised or unlawful access, disclosure, alteration, loss, or destruction, as further described in the Data Processing Agreement and Annex 1 (Technical and Organisational Measures). Such measures shall be appropriate to the nature of the Services and the risks presented by the processing activities undertaken by the Provider.

3.8 Third-Party Access

The Customer may permit authorised third parties to access the Platform only where:

- such access is reasonably necessary for the Customer's legitimate business purposes and complies with this Agreement;
- the Provider has approved such access where the third party is a software developer, integration provider, consultant, contractor, or managed service provider;
- each third party is assigned an individual named user account and unique authentication credentials;
- the Customer ensures that appropriate role-based access controls ("RBAC") are applied and maintained for all third-party users;
- all third-party access activity is subject to logging, monitoring, and audit controls maintained by the Platform;
- the third party is bound by confidentiality obligations and acceptable-use restrictions no less protective than those contained in this Agreement and the Acceptable Use Policy; and
- the Customer promptly revokes access when no longer required.

The Customer remains fully responsible and liable for all acts, omissions, and use of the Platform by any third party accessing the Platform through the Customer's account or under the Customer's authority.

The Customer must not permit the sharing of user accounts, shared login credentials, or generic access credentials except where expressly authorised by the Provider in writing for a specific operational purpose.

3.9 Sub-Licensing of the Platform

The Customer may permit approved Affiliates or authorised third parties to access and use the Platform within the scope expressly authorised in the applicable Order Form, provided that:

(a) the Provider gives prior written consent, such consent not to be unreasonably withheld or delayed;

(b) any approved sub-licence or third-party access is limited to the Customer's internal business operations and permitted use of the Platform;

(c) the Customer remains fully responsible and liable for all acts, omissions, access, use, processing activities, and breaches by any sub-licensee, Affiliate, contractor, consultant, integration provider, managed service provider, or other third party accessing the Platform through or on behalf of the Customer;

(d) the Customer shall ensure that all sub-licensees and authorised third parties are bound by written obligations relating to confidentiality, security, acceptable use, data protection, and access controls that are no less protective than those contained in this Agreement, the Acceptable Use Policy, and the Data Processing Agreement;

(e) all users accessing the Platform under any sub-licence must use individual named user accounts and unique authentication credentials, and the Customer shall ensure appropriate role-based access controls and prompt removal of unnecessary access rights;

(f) the Customer shall ensure that any processing of Personal Data by a sub-licensee or authorised third party complies with applicable Data Protection Laws and does not cause the Provider to breach applicable law or regulatory obligations;

(g) the Provider may suspend, restrict, or terminate any approved sub-licensed access where reasonably necessary for security, operational, legal, regulatory, or compliance reasons; and

(h) any additional Fees applicable to approved sub-licensing arrangements shall be reflected in the applicable Order Form.

The Customer must not permit shared accounts, generic credentials, uncontrolled onward access, or any use of the Platform that would compete with, replicate, resell, or commercially exploit the Platform except as expressly authorised in writing by the Provider.

3.10 Add-On Features

- The Provider may offer Add-On Features that enhance the functionality of the Platform. The Customer may choose to subscribe to Add-On Features for an additional Fee. The use of such Add-On Features shall be subject to the terms of this Agreement and any applicable Supplemental Terms agreed upon at the time of subscription in the Order Form. Add-On Features may have different renewal terms and may be discontinued at the Provider's sole discretion.

3.11 Beta Services

- From time to time, the Provider may offer early access to new features or functionalities of the Platform ("Beta Services"). Beta Services are provided for testing and evaluation purposes only, and the Provider reserves the right to modify or discontinue Beta Services at any time without notice. The Customer acknowledges that Beta Services may be incomplete, contain Defects, or not function as intended. The Provider makes no warranties regarding Beta Services, and the Customer's use of Beta Services is at its own risk.

3.12 AI Functionality

Certain aspects of the Platform include artificial intelligence or machine learning capabilities ("AI Functionality"). AI Functionality forms part of the Services and provides AI-assisted workflow support within the Platform, including functionality designed to assist with drafting, summarisation, recommendations, operational workflows, and other user-support activities made available within the Services from time to time.

Unless expressly agreed otherwise in writing by BrokerCentral, AI Functionality may be made available within normal Platform workflows and is not a separately disableable service or optional add-on at Customer level. The Customer is not required to rely on AI-generated outputs, and Authorised Users may choose not to accept or use AI-generated suggestions, recommendations, drafts, summaries, or other outputs.

The Customer acknowledges that AI-generated outputs may not always be accurate, complete, reliable, current, legally compliant, non-discriminatory, or suitable for the Customer's intended use. The Customer and its Authorised Users are responsible for reviewing, verifying, and validating all AI-generated outputs before accepting, applying, sending, publishing, recording, or otherwise relying on them.

Unless expressly agreed otherwise in writing by BrokerCentral, AI Functionality is provided solely as a decision-support tool and is not intended to operate as a fully automated decision-making system. AI-generated outputs must not be used as the sole basis for regulated, legal, financial, insurance, employment, customer-facing, compliance, or similarly significant decisions. The Customer must ensure that appropriately qualified personnel apply meaningful human review, verification, and professional judgment before using or relying on AI-generated outputs in any such context.

The Customer shall ensure that AI Functionality is used in a lawful, fair, transparent, and accountable manner consistent with applicable Data Protection Laws and any applicable laws, regulations, or regulatory guidance relating to automated processing, profiling, artificial intelligence, discrimination, consumer protection, insurance, financial services, PECR, cookies, similar tracking technologies, electronic marketing communications, or electronic communications.

The Customer must not use AI Functionality:

- as the sole basis for decisions producing legal effects concerning an individual, similarly significant effects, or regulated, legal, financial, insurance, employment, customer-facing, compliance, or similarly significant outcomes;
- in a manner that is discriminatory, unfair, deceptive, misleading, defamatory, unlawful, or harmful;
- to process Personal Data in breach of applicable Data Protection Laws;
- to generate unlawful profiling, behavioural analysis, automated risk scoring, behavioural monitoring, or Tracking Technology-related processing contrary to applicable law, PECR, or regulatory guidance; or
- in connection with prohibited activities identified in the Acceptable Use Policy.

The Customer acknowledges that:

- AI-generated outputs may reflect limitations inherent in statistical and machine-learning systems;
- outputs may vary over time;
- AI outputs may require independent verification and contextual review;
- AI systems may produce inaccurate, incomplete, biased, or unexpected outputs; and
- meaningful human review and oversight should be applied before relying on AI-generated outputs in operational, financial, insurance, compliance, legal, employment, customer-facing, profiling, marketing, or communications contexts.

The Provider may implement operational, technical, security, monitoring, filtering, rate-limiting, logging, review, or governance controls relating to AI Functionality where reasonably necessary to:

- comply with applicable law, PECR, or regulatory obligations;
- protect platform security or integrity;
- reduce operational or legal risk;
- prevent misuse, abusive activity, unlawful tracking, or unlawful electronic communications activity; or
- support responsible AI governance practices.

The Customer shall ensure that appropriately qualified personnel exercise meaningful human review and oversight over any decisions, actions, recommendations, or outputs generated using AI Functionality where such decisions may:

- produce legal effects concerning an individual; or
- otherwise have a material, financial, regulatory, employment, insurance, or similarly significant impact on any person or organisation.

The Customer remains solely responsible for:

- all decisions made using AI Functionality;
- compliance with applicable laws and regulations relating to automated decision-making, discrimination, consumer protection, insurance, financial services, data protection, PECR, Tracking Technologies, cookies, electronic marketing communications, and electronic communications; and
- ensuring that AI-generated outputs are not used in a misleading, discriminatory, unlawful, harmful, or privacy-invasive manner.

The Provider does not use Customer Data, Customer Personal Data, prompts or outputs to train public or shared AI models, and contractually restricts relevant AI providers from doing so, unless expressly agreed in writing.

Where AI Functionality relies on third-party AI service providers, the Customer acknowledges that relevant input and output data may be processed by such providers in accordance with applicable data protection laws, PECR where applicable, and the Provider's agreements with those providers.

The Provider reserves the right to suspend, restrict, modify, or withdraw AI Functionality where reasonably necessary to address legal, regulatory, ethical, security, operational, privacy, Tracking Technology, electronic communications, or third-party provider requirements.

4. SUPPORT SERVICES AND UPGRADES

4.1 Support Services

- During the Subscription, the Provider shall provide Support Services to the Customer and may apply Upgrades to the Platform, in accordance with the service level agreement set out in Schedule 1.

4.2 Sub-Contracting Support Services

The Provider may sub-contract the provision of Support Services and other operational services without obtaining prior consent from the Customer, provided that:

- where any subcontractor processes Personal Data on behalf of the Customer, such subcontractor shall be treated as a Sub-Processor under the Data Processing Agreement;
- the Provider shall ensure that such subcontractors are subject to written obligations no less protective than those set out in the Data Processing Agreement; and
- the Provider shall remain responsible for the acts and omissions of its subcontractors in connection with the provision of the Services to the same extent that the Provider would be responsible if it performed the relevant obligations itself, subject to the exclusions, limitations, and liability caps set out in this Agreement.

5. CUSTOMER MATERIALS AND INTELLECTUAL PROPERTY RIGHTS

5.1 Licence to Use Customer Materials

The Customer grants the Provider, during the Subscription, a non-exclusive, worldwide, royalty-free licence to host, store, process, transmit, copy, and otherwise use the Customer Materials solely to the extent necessary to:

- provide, operate, secure, maintain, and support the Platform and Services;
- perform the Provider's obligations and exercise its rights under this Agreement;
- comply with applicable law, regulatory obligations, or lawful requests from public authorities;
- prevent fraud, security threats, or misuse of the Platform; and
- generate service analytics, operational telemetry, usage statistics, performance metrics, and related operational information relating to the Platform and Services, provided that:
    - any Personal Data is processed in accordance with the Data Processing Agreement and the Customer's documented instructions;
    - such analytics are used only for the Provider's internal business operations, service administration, security, billing, capacity planning, and service improvement purposes; and
    - any data disclosed externally or used across customers is aggregated and anonymised using measures designed to prevent the identification or re-identification of any Customer, individual, or Personal Data by means reasonably likely to be used; and
    - the Provider shall not knowingly attempt to re-identify anonymised data.

Nothing in this Agreement grants the Provider any right to:

- sell Customer Materials;
- use Customer Personal Data to train public or shared machine learning models; or
- process Personal Data for its own independent commercial purposes except where the Provider acts as an independent controller under applicable law.

To the extent the Provider processes Personal Data contained within Customer Materials on behalf of the Customer, such processing shall be governed exclusively by the Data Processing Agreement.

5.2 Ownership of Customer Materials

- Subject to Clause 5.1, all Intellectual Property Rights in the Customer Materials shall remain, as between the parties, the exclusive property of the Customer.

5.3 Warranties Regarding Customer Materials

- The Customer warrants and represents to the Provider that the Customer Materials, and their use by the Provider in accordance with this Agreement, shall not:

    (a) Breach any applicable laws, regulations, or legally binding codes;

    (b) Infringe any third party's Intellectual Property Rights or other legal rights; or

    (c) Give rise to any claim, legal action, or liability against the Provider, the Customer, or any third party.

5.4 Provider's Rights on Suspected Breaches

- If the Provider reasonably suspects that the Customer has breached any provisions of Clause 5, the Provider may, without liability:

    (a) Remove, modify, or restrict access to the relevant Customer Materials; and/or

    (b) Suspend some or all of the Services and/or the Customer's access to the Platform while investigating the matter.

5.5 Material Breach

- A breach of Clause 5 by the Customer shall be deemed a material breach of this Agreement for the purposes of Clause 13 (Termination).

5.6 Intellectual Property Rights of the Platform and Services

- The Provider and/or its licensors retain all Intellectual Property Rights in and to:

  (a) The Platform, including any customisations, modifications, or enhancements made by or for the Provider;

  (b) The Services, including any support, updates, or additional features;

  (c) The Documentation; and

  (d) Any Additional Projects developed or delivered by the Provider.

- Except as expressly granted in this Agreement, the Customer does not acquire any rights, title, or interest in or to the Platform, Services, Documentation, or Additional Projects.

6. RESERVED.

7. CHARGES AND FEES

7.1 Invoicing and Payment Obligations

- The Provider shall issue invoices for the Charges and Fees to the Customer in accordance with the provisions of the Order Form.
- The Customer agrees to pay all invoiced amounts in full within seven (7) days of the invoice date, using a bank transfer or any other approved payment method notified by the Provider.

7.2 Taxes and Withholding

- All Charges and Fees are exclusive of applicable taxes. The Customer shall pay any VAT, sales tax, or other applicable levies in addition to the principal amounts.
- If withholding tax applies, the Customer must gross up payments so that the full invoice amount is received by the Provider.

7.3 Payment Methods

- The Customer shall pay via bank transfer or other payment methods approved by the Provider, using the details provided.

7.4 Late Payments and Interest

If the Customer fails to pay any undisputed amount due under this Agreement by the applicable due date, the Provider may:

(a) charge interest on the overdue amount at the statutory rate applicable under the Late Payment of Commercial Debts (Interest) Act 1998, accruing daily from the due date until payment is made in full;

(b) recover fixed compensation, reasonable debt recovery costs, administrative costs, legal costs, and collection costs to the extent permitted under applicable law;

(c) suspend or restrict access to the Platform and Services in accordance with Clause 7.6 until all overdue undisputed amounts are paid; and

(d) charge reasonable reactivation, administration, storage, recovery, or restoration fees associated with restoring suspended Services.

The Provider's rights under this Clause are without prejudice to any other rights or remedies available under this Agreement or applicable law.

Where the Late Payment of Commercial Debts (Interest) Act 1998 does not apply, the Provider may charge interest on overdue undisputed amounts at a rate of eight percent (8%) per annum above the Bank of England base rate, accruing daily from the due date until payment is made in full.

7.5 Adjustment of Fees

Unless otherwise stated in the applicable Order Form, the Provider may increase recurring Subscription Fees once in each twelve (12) month period by an amount not exceeding the percentage increase in the UK Consumer Prices Index over the relevant period.

The Provider shall give the Customer reasonable written notice of any annual CPI-based Fee increase before it takes effect.

Except for annual CPI-based increases permitted under this Clause 7.5, increases expressly stated in the applicable Order Form, or increases otherwise agreed in writing by the Customer, the Provider shall not increase recurring Subscription Fees during the then-current Subscription Term.

The Provider may charge additional Fees for Add-On Features, New Functionality, Additional Projects, increased usage, additional users, upgraded entitlements, support services, professional services, premium services, bespoke modifications, customer-requested enhancements, restoration requests, migration assistance, or other chargeable services where such items are ordered, enabled, agreed to, requested, or used by the Customer in accordance with this Agreement, the applicable Order Form, the purchase process, or other written agreement.

Nothing in this Clause prevents the Provider from charging Fees or Charges already contemplated by this Agreement, including Charges for Additional Projects, Add-On Features, restoration work, migration assistance, overdue payment recovery, or usage exceeding the Customer's agreed Subscription plan.

7.6 Non-Payment and Suspension of Services

If any undisputed payment remains overdue for more than fifteen (15) days, the Provider may, upon written notice and without liability:

- suspend or restrict the Customer's access to the Platform and Services;
- suspend processing activities that are not legally or operationally required;
- restrict access to non-essential functionality; and
- charge reasonable reactivation, administration, storage, or recovery fees associated with restoring suspended Services.

During any suspension period, the Provider shall retain Customer Materials securely in accordance with the Data Processing Agreement and applicable law.

The Provider shall not permanently delete Customer Materials solely due to non-payment except:

- where required by applicable law;
- where retention would create a legal, regulatory, or security risk; or
- following expiration of applicable post-termination retention periods under the Agreement and Data Processing Agreement.

Subject to payment of reasonable applicable fees and compliance with law, the Customer may request export of its Customer Materials during the applicable retention period in a commonly used machine-readable format.

7.7 Subscription Commitment

- Unless explicitly agreed otherwise, the Customer remains liable for all Licence Fees until the expiry of the Subscription, even if the Platform or Services are not used.

8. WARRANTIES

8.1 Customer Warranties

The Customer warrants that:

(a) It has the legal right and authority to enter into this Agreement and use the Platform in accordance with the Permitted Purpose.

(b) It is solely responsible for ensuring compliance with financial services legislation and regulations applicable to its business.

8.2 Provider Warranties

The Provider warrants that:

(a) It has the legal right and authority to enter into and perform its obligations under this Agreement.

(b) It will provide the Platform and Support Services with reasonable care and skill.

(c) The Platform will substantially perform as described in the Documentation, subject to any Upgrades.

(d) The Platform will be hosted in accordance with commitments set out in Schedule 1.

(e) The Platform (excluding Customer Materials) does not infringe any third-party Intellectual Property Rights.

8.3 Service Limitations

The Customer acknowledges and agrees that:

- The Customer acknowledges and agrees that:

(a) except as expressly set out in this Agreement, the Platform and Services are provided on an “as available” basis;

(b) while the Provider will use commercially reasonable efforts to maintain the availability, security, and functionality of the Platform in accordance with this Agreement and Schedule 1, the Provider does not warrant that the Platform will be uninterrupted, error-free, or completely free from Defects;

(c) the Platform may not be compatible with all third-party applications, systems, integrations, or software unless expressly stated in the applicable Order Form or Documentation;

(d) the Provider is not responsible for issues, failures, delays, vulnerabilities, or disruptions arising from:

(i) third-party integrations, applications, or services not controlled by the Provider;
(ii) Customer systems, infrastructure, internet connectivity, or configurations;
(iii) Customer misuse, unauthorised modifications, or use outside the Permitted Purpose; or
(iv) Beta Services, evaluation features, or third-party software made available on a non-production basis; and

(e) except to the extent prohibited by applicable law, all warranties, representations, conditions, and other terms not expressly set out in this Agreement are excluded to the fullest extent permitted by law.

8.4 Exclusions and Limitations

- The warranties in Clause 8.2 do not apply to:

(a) non-conformities, interruptions, or issues arising from Customer modifications, misuse, negligence, unauthorised access, or use of the Platform contrary to this Agreement or the Documentation;

(b) downtime, latency, interruptions, or failures caused by internet service providers, telecommunications networks, hosting providers, cloud infrastructure providers, or other third-party dependencies outside the Provider's reasonable control;

(c) issues arising from third-party integrations, applications, APIs, or software not supplied or controlled by the Provider; or

(d) the Customer's business operations, regulatory obligations, financial transactions, underwriting decisions, compliance activities, or operational decisions made using the Platform or AI Functionality.

8.5 Indemnification for Third-Party Claims

(a) If a third party claims that the Platform infringes its Intellectual Property Rights, the Provider will, at its discretion:

- Obtain rights for the Customer to continue using the Platform;
- Modify the Platform to be non-infringing; or
- Terminate the Agreement and provide a prorated refund of any Fees already paid for the unused portion of the Subscription Term from the termination date.

(b) The Provider will have no obligation under Clause 8.5 if the claim results from:

- Customer Materials;
- Customer's unauthorised modifications to the Platform;
- Customer's misuse of the Platform in a manner not intended under this Agreement.

9. INDEMNITIES

9.1 Customer Indemnification

The Customer shall indemnify, defend, and hold harmless the Provider, its Affiliates, officers, directors, employees, and agents from and against any liabilities, damages, losses, costs, and expenses (including legal fees) arising out of:

(a) The Customer's breach of Clause 5.3 (Intellectual Property Rights of Customer Materials) or any other clause in this Agreement;

(b) The Customer's misuse of the Platform, including violations of statutory, regulatory, or contractual obligations;

(c) Any third-party claims arising from the Customer's data, including privacy violations, intellectual property disputes, or unauthorised data usage;

(d) Security breaches, data loss, or unauthorised access resulting from the Customer's failure to maintain adequate security measures for its credentials, data, or systems;

(e) Any claims arising from third-party software, integrations, or applications not provided by the Provider and used by the Customer, where such claims result from incompatibility, security risks, or unauthorised modifications made to the Platform.

(f) any claims, penalties, fines, losses, damages, liabilities, costs, or expenses arising from the Customer's breach of applicable Data Protection Laws, the Data Processing Agreement, unlawful processing instructions, failure to provide required privacy notices, failure to obtain required consents or lawful bases, or other acts or omissions for which the Customer is responsible under the Data Processing Agreement.

9.2 Provider Indemnification

The Provider shall indemnify, defend, and hold harmless the Customer against any third-party claim arising out of a breach of Clause 8.2(e) (Intellectual Property Rights infringement), subject to the following conditions:

(a) The Customer must provide prompt written notice of any claim;

(b) The Customer must cooperate reasonably in the defense of the claim, at the Provider's expense;

(c) The Provider has sole authority to defend or settle the claim.

In response to such a claim, the Provider may, at its discretion:

(i) Procure the right for the Customer to continue using the Platform;

(ii) Modify or replace the Platform to avoid infringement; or

(iii) If neither option (i) nor (ii) is commercially reasonable or feasible, terminate this Agreement and provide a pro-rata refund of Subscription Fees already paid for the unused period of the Subscription Term.

9.3 Indemnity Exclusions

The Provider will not be liable for any claims arising from:

(a) Customer modifications to the Platform, including customisations, alterations, or third-party integrations added without the Provider's prior written consent;

(b) Customer use of the Platform contrary to instructions or outside the scope of permitted use;

(c) Customer's continued use of the Platform after an infringement notice;

(d) Security breaches, hacking, or unauthorised access caused by Customer negligence, lack of security controls, or failure to implement recommended updates;

(e) Third-party software, applications, or integrations that are not provided or maintained by the Provider, even if they interoperate with the Platform;

(f) Any claim based on the combination of the Platform with other software or services, where such combination causes infringement, malfunction, or security vulnerabilities.

9.4 Security and Third-Party Integration Disclaimer

(a) The Customer acknowledges that third-party integrations, applications not provided by the Provider, and external APIs may introduce security risks, data loss, or service disruptions, and that the Provider is not responsible for any resulting liabilities.

(b) The Customer is responsible for assessing the security, compliance, and reliability of any third-party integration before enabling it for use with the Platform.

(c) The Provider may, at its discretion, suspend or disable third-party integrations that pose a security or legal risk to the Platform, Services, or other Customers.

9.5 Sole Remedy

- The remedies described in Clauses 9.1 to 9.4 constitute the Customer's exclusive remedy for any third-party claims, data security issues, or intellectual property infringement claims.

9.6 Open-Source Software Disclaimer

- The Customer acknowledges that any Open-Source Software provided by the Provider is supplied "as is", without warranties, and subject to the disclaimer in Clause 8.3. The Platform may include Open-Source Software under various licenses (including but not limited to MIT, GPL, Apache). The Provider shall comply with all applicable Open-Source License obligations and will disclose modifications upon request.

9.7 Limitation of Indemnity Liability

Except to the extent prohibited by applicable law, all indemnities under this Agreement shall be subject to the limitations and exclusions of liability set out in Clause 10.

10. LIMITATIONS AND EXCLUSIONS OF LIABILITY

10.1 Non-Excludable Liability

Nothing in this Agreement shall:

(a) Limit or exclude a party's liability for death or personal injury caused by negligence;

(b) Limit or exclude a party's liability for fraud or fraudulent misrepresentation;

(c) Limit liability in a manner that is not permitted under applicable law; or

(d) Exclude liability that cannot legally be excluded.

10.2 Scope of Liability Limitation

- The limitations and exclusions in this Clause apply to all liabilities arising under this Agreement, including those arising in contract, tort (including negligence), statutory duty, or otherwise.

10.3 Cap on Liability

(a) Subject to Clauses 10.1 and 10.3(b), each party's aggregate liability arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total Charges and Fees paid or payable by the Customer under this Agreement during the six (6) months immediately preceding the event giving rise to the claim.

(b) The aggregate liability of either party arising from:

- breach of confidentiality obligations;
- breach of applicable data protection laws;
- Personal Data Breaches;
- security incidents caused by a party's failure to implement reasonable security measures; or
- indemnification obligations under Clause 9, shall not exceed the total Charges and Fees paid or payable by the Customer under this Agreement during the twelve (12) months immediately preceding the event giving rise to the claim.

(c) The limitations in this Clause 10.3 apply collectively to all claims arising under or in connection with this Agreement and are not cumulative.

10.4 Exclusion of Indirect and Consequential Damages

To the maximum extent permitted by law, under no circumstances will either party be liable to the other for:

(a) Third-party claims against the party for loss or damages;

(b) loss, corruption, destruction, alteration, unauthorised disclosure, or unavailability of the Customer's records, data, or Customer Materials, except to the extent directly caused by the Provider's failure to implement the security measures, backup procedures, or data protection obligations expressly required under this Agreement or the Data Processing Agreement, in which case the Provider's liability shall remain subject to the limitations, exclusions, and liability caps set out in this Agreement.

(c) Loss of profit, revenue, goodwill, or anticipated savings (whether direct or indirect);

(d) Business interruption, lost opportunities, reputational damage, or increased costs;

(e) Any special, indirect, incidental, or consequential loss or damage, whether foreseeable or not, arising in connection with this Agreement.

For the avoidance of doubt, the Provider's obligations relating to backup procedures, restoration efforts, Personal Data security, and Personal Data Breaches are governed by this Agreement, the Data Processing Agreement, and Schedule 1, and nothing in this Clause 10.4 excludes liability that cannot lawfully be excluded under applicable Data Protection Laws.

10.5 Service Availability, Third-Party Applications, and Integrations

(a) Service Availability
The Provider does not guarantee uninterrupted or error-free service. The Customer acknowledges that occasional disruptions, maintenance, or third-party dependencies may impact service availability.

(b) Third-Party Applications & Integrations
The Provider shall not be liable for any damages, loss, or disruptions caused by:

- Customer's use of third-party software, APIs, or applications not provided by the Provider, even if integrated with the Platform.
- Errors, incompatibilities, or failures arising from the interaction of the Platform with third-party software or systems.
- Data loss, security breaches, or performance issues resulting from third-party integrations, including but not limited to external authentication tools, analytics platforms, payment gateways, or automation software.
- Tracking Technologies, telemetry systems, analytics technologies, cookies, pixels, scripts, or similar technologies deployed through third-party integrations or applications;
- Downtime, modifications, or discontinuation of a third-party service that affects the Platform's functionality.
- Customer's reliance on third-party tools, recommendations, or add-ons, whether provided through the Provider's marketplace, API integrations, or other means.

(c) Third-Party Data Processing Risks
The Provider shall not be liable for any data breaches, unauthorised disclosures, or regulatory violations arising from the Customer's use of third-party data processing services, cloud storage solutions, or external applications.

(d) Security Responsibilities for Third-Party Applications

(i) The Customer is responsible for assessing the security, compliance, and reliability of any third-party integration before enabling it for use with the Platform.

(ii) The Provider does not guarantee that third-party integrations will comply with privacy laws, data protection regulations, or industry standards.

(iii) The Customer shall indemnify the Provider for any liability, claims, or regulatory fines arising from the Customer's reliance on third-party applications or failure to implement appropriate security measures.

(e) Provider's Right to Suspend Third-Party Integrations
The Provider may, at its sole discretion, suspend or disable any third-party integrations that pose a security, legal, or operational risk to the Platform, Services, or other Customers.

10.6 AI-Generated Content and Functionality

(a) No Guarantee of Accuracy

The Provider makes no warranties regarding the accuracy, reliability, suitability, completeness, legality, or availability of any AI-generated content, recommendations, analyses, insights, or outputs generated through AI-powered functionality within the Platform.

The Customer acknowledges that AI-generated outputs are based on statistical and machine-learning models and may contain errors, inaccuracies, biases, omissions, hallucinations, or incomplete information.

AI-generated outputs may be probabilistic in nature and may vary depending on prompts, contextual inputs, training limitations, third-party model behaviour, system configurations, and evolving technologies.

The Provider does not represent or warrant that AI-generated outputs will:

- be accurate, complete, reliable, or error-free;
- be explainable or interpretable;
- be legally or regulatorily compliant;
- be free from bias or discriminatory outcomes; or
- be suitable for any regulated, high-risk, or legally significant use case without independent human review and validation.

(b) Customer's Responsibility for AI Use

(i) The Customer is solely responsible for reviewing, validating, verifying, and assessing all AI-generated outputs before relying on them for any business, financial, legal, insurance, underwriting, compliance, employment, operational, or regulatory purpose.

(ii) The Customer must ensure that its use of AI Functionality and AI-generated outputs complies with:

- applicable laws;
- regulatory requirements;
- contractual obligations;
- industry standards; and
- applicable Data Protection Laws, including requirements relating to automated decision-making, profiling, discrimination, consumer protection, insurance regulation, PECR, Tracking Technologies, electronic communications, privacy, marketing communications, and cybersecurity.

(iii) The Customer acknowledges that AI Functionality is intended to support, and not replace, human judgment unless expressly agreed otherwise in writing by the Provider.

(iv) The Customer must ensure that appropriately qualified personnel exercise meaningful human oversight and review over any AI-assisted process, recommendation, output, or decision that may materially affect individuals, customers, transactions, underwriting decisions, claims handling, compliance activities, employment matters, or other legally or commercially significant outcomes.

(v) The Provider is not liable for any legal claims, regulatory penalties, enforcement action, business losses, reputational harm, or other liabilities resulting from:

- the Customer's reliance on AI-generated outputs;
- the Customer's failure to implement appropriate human oversight;
- the Customer's unlawful or inappropriate use of AI Functionality; or
- decisions made by the Customer based on AI-generated outputs.

(vi) The Customer acknowledges that the Platform may display notices, prompts, warnings, confirmation steps, or similar controls reminding Authorised Users to check AI-generated outputs before use. Such notices are intended to support responsible use of AI Functionality and do not reduce the Customer's responsibility to ensure that appropriately qualified personnel review, verify, and validate AI-generated outputs before relying on them.

(c) AI Training and Data Use

(i) The Provider does not use Customer Data, Customer Personal Data, prompts or outputs to train public or shared AI models, and contractually restricts relevant AI providers from doing so, unless expressly agreed in writing.

(ii) If AI Functionality involves third-party AI service providers, the Customer acknowledges and agrees that relevant input and output data may be processed by such providers in accordance with:

- applicable Data Protection Laws;
- the Provider's agreements with such providers; and
- applicable third-party terms governing the relevant AI services.

(iii) The Provider may use anonymised and aggregated operational telemetry, service analytics, security metrics, usage statistics, and performance data for:

- internal service improvement;
- security and fraud prevention;
- reliability and operational monitoring;
- capacity planning; and
- platform optimisation purposes, provided that such information does not reasonably identify the Customer or any individual.

(d) AI Restrictions

The Customer must not use AI Functionality:

(i) to generate deceptive, fraudulent, defamatory, unlawful, harmful, discriminatory, harassing, or misleading content;

(ii) to conduct unlawful profiling, behavioural analysis, or automated risk scoring;

(iii) to create fully automated decisions producing legal effects concerning an individual, or similarly significant effects, without appropriate lawful basis, safeguards, and meaningful human oversight;

(iv) in any manner that violates applicable:

- Data Protection Laws;
- PECR;
- privacy laws;
- Tracking Technologies or cookie requirements;
- electronic communications laws;
- discrimination laws;
- insurance regulations; or
- financial services regulations;

(v) to circumvent legal, regulatory, audit, compliance, or security controls;

(vi) to process Special Category Data unlawfully; or

(vii) in connection with any activity prohibited under the Acceptable Use Policy.

(e) Regulatory and Operational Controls

The Provider may implement monitoring, filtering, moderation, logging, rate limiting, suspension, restriction, governance, or operational controls relating to AI Functionality where reasonably necessary to:

- comply with applicable law, regulatory obligations, or lawful requests;
- address security, abuse, fraud, or operational risks;
- comply with third-party AI provider requirements;
- support responsible AI governance practices; or
- protect the Platform, Services, Provider, Customers, or third parties.

(f) Right to Modify or Withdraw AI Functionality

The Provider reserves the right to suspend, restrict, modify, discontinue, or withdraw AI Functionality where reasonably necessary for legal, regulatory, ethical, operational, security, technical, or third-party dependency reasons.

10.7 Regulatory Compliance and Risk Allocation

- **(a) Customer's Regulatory Obligations**
  The Customer is solely responsible for ensuring that:
  - Its business operations comply with financial services laws, data protection regulations, and industry standards.
  - Its use of the Platform, including AI functionality, does not violate legal or contractual obligations.
  - All transactions, communications, or business processes conducted via the Platform comply with applicable regulatory frameworks.
- **(b) No Provider Liability for Regulatory Breaches**
  The Provider shall not be liable for:
  - Regulatory fines, enforcement actions, or third-party claims arising from the Customer's non-compliance with laws or industry standards;
  - Any reliance on AI-generated insights, predictions, or risk assessments that do not align with legal, financial, or compliance requirements;
  - Customer decisions or transactions made through the Platform that result in regulatory non-compliance.
- **(c) Suspension for Regulatory Non-Compliance**
  The Provider reserves the right to suspend or terminate access to the Platform or specific functionalities if required to comply with legal, regulatory, or law enforcement orders.

11. DATA PROTECTION

11.1 Customer Warranties and Responsibilities

- The Customer warrants that it has the legal right to disclose all Personal Data provided to the Provider under or in connection with this Agreement. The Customer shall ensure that its collection, use, disclosure, storage, transfer, and other processing of Personal Data comply with applicable Data Protection Laws, including requirements relating to transparency, lawful basis, PECR, Tracking Technologies, cookies, electronic communications, marketing communications, international transfers, automated decision-making, and security obligations, as further described in the Data Processing Agreement (DPA).

11.2 Provider Warranties and Data Processing Obligations

- The Provider shall process Personal Data strictly in accordance with the Data Processing Agreement (DPA). This includes compliance with applicable Data Protection Laws relating to security obligations, breach notifications, international transfers, complaint handling, lawful processing, electronic communications, records management, and regulatory cooperation.

11.3 Data Security Measures

- All security measures related to data processing, including encryption, access controls, and incident response, shall be implemented in accordance with the Data Processing Agreement (DPA). The Provider shall maintain appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of Personal Data. Such measures may be updated from time to time to reflect changes in applicable Data Protection Laws, regulatory guidance, industry standards, security threats, and operational risk assessments.

11.4 Data Breach Notification

- In the event of a Personal Data Breach, the Provider shall notify the Customer in accordance with the Data Processing Agreement (DPA). The notification shall include details on the nature of the breach, affected data categories, and mitigation measures including obligations arising under applicable Data Protection Laws relating to Personal Data Breaches, security incidents, and regulatory notification requirements..

11.5 Data Processing Roles and Responsibilities

- Except where otherwise expressly stated, the Provider shall act as a processor and the Customer shall act as a controller (or equivalent concepts under applicable Data Protection Laws) in relation to Personal Data processed on behalf of the Customer. The obligations related to processing, compliance, and regulatory requirements are governed by the DPA. Disputes regarding Data Processing shall be governed under the laws of England and Wales, consistent with the DPA.

11.6 International Data Transfers

The Provider shall not transfer, access, process, store, disclose, or otherwise make available Personal Data outside the United Kingdom or any jurisdiction subject to applicable international transfer restrictions unless such transfer complies with the Data Processing Agreement (DPA) and applicable Data Protection Laws.

Where restricted international transfers occur, the Provider shall implement lawful transfer mechanisms and appropriate technical, contractual, and organisational safeguards recognised under applicable Data Protection Laws, which may include:

- adequacy regulations or adequacy decisions;
- the International Data Transfer Agreement (“IDTA”);
- the UK Addendum to the EU Standard Contractual Clauses;
- EU Standard Contractual Clauses (“EU SCCs”);
- recognised certification or transfer frameworks, including the UK-US Data Bridge where applicable;
- Binding Corporate Rules (“BCRs”); or
- other lawful transfer mechanisms, derogations, or safeguards permitted under applicable Data Protection Laws.

The Provider may update, replace, supplement, or adopt alternative transfer mechanisms or safeguards where reasonably necessary to:

- comply with applicable law, regulatory guidance, or supervisory authority requirements;
- reflect changes in recognised transfer frameworks or adequacy decisions;
- address operational, technical, security, or infrastructure requirements; or
- maintain lawful international transfer arrangements.

Where required under applicable Data Protection Laws, the Provider may conduct and maintain transfer risk assessments, vendor due diligence assessments, and supplementary technical and organisational safeguards relating to international transfers of Personal Data.

11.7 Use of Sub-Processors

- The engagement of sub-processors, including notification requirements and liability, shall be governed by the Data Processing Agreement (DPA). The Customer retains the right to object to new sub-processors under the conditions outlined in the DPA including AI service providers processing Personal Data in connection with AI Functionality.

11.8 Data Retention and Deletion

- Upon termination or expiration of this Agreement, the Provider shall delete or return all Personal Data in accordance with the Data Processing Agreement (DPA) and any applicable legal, regulatory, audit, security, backup, disaster recovery, or operational retention obligations. If the Customer requires data retrieval post-termination, a request must be made within the period specified in the DPA.

12. CONFIDENTIALITY

12.1 Definition of Confidential Information

"Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes but is not limited to:

- Customer Confidential Information, including business strategies, pricing structures, proprietary methodologies, and financial details.
- Technical information, including software, designs, product plans, source code, algorithms, trade secrets, and data structures.
- Personal Data, as defined in the Data Processing Agreement (DPA), including any Customer Materials containing personally identifiable information (PII) or other regulated data.
- Platform details, including its architecture, security measures, and operational mechanisms.

12.2 Obligations of Confidentiality

The Receiving Party shall:

(a) Maintain the confidentiality of the Disclosing Party's Confidential Information using at least the same degree of care that it uses to protect its own confidential information of a similar nature, but in no event less than reasonable care in accordance with industry standards.

(b) Not disclose the Confidential Information to any third party without the prior written consent of the Disclosing Party, except as permitted under Clause 12.3.

(c) Use the Confidential Information solely for the purpose of fulfilling its obligations under this Agreement.

12.3 Permitted Disclosures

Confidential Information may be disclosed only in the following circumstances:

(a) To employees, affiliates, officers, agents, insurers, or professional advisers who need to know such information to perform obligations under this Agreement, provided they are bound by similar confidentiality obligations.

(b) If required by law, regulation, court order, or regulatory authority, provided that the Receiving Party:

- Gives prompt written notice (if legally permissible) to the Disclosing Party before disclosure;
- Provides reasonable assistance to the Disclosing Party in opposing or limiting the disclosure.

- (c) If the Confidential Information:
  - Becomes publicly known without breach of this Agreement;
  - Was lawfully in possession of the Receiving Party prior to disclosure;
  - Was independently developed by the Receiving Party without reference to the Confidential Information;
  - Was disclosed by a third party without obligation of confidentiality.

12.4 Data Retention and Post-Termination Obligations

(a) Upon termination of this Agreement, the Receiving Party shall:

- Irrevocably delete Confidential Information stored electronically, unless required to be retained under applicable law.
- Return or destroy all physical copies of Confidential Information.
- Upon request, provide written certification of compliance with these obligations.

(b) **Retention in Routine Backups**

- Notwithstanding Clause 12.4(a), the Receiving Party may retain Confidential Information in routine backups that are created as part of standard business continuity procedures.
- Any such Confidential Information retained in backups shall remain subject to the confidentiality obligations of this Agreement.
- Confidential Information in backups shall not be actively used, disclosed, or restored except as required for disaster recovery or compliance purposes.
- Such backups will be deleted in accordance with the Receiving Party's standard retention policies, provided that:
  - The backup cycle does not retain data longer than necessary for operational continuity.
  - The Receiving Party ensures that such backups remain secure and inaccessible for general business use.

(c) **Compliance with Data Processing Agreement (DPA):**
The Receiving Party's obligations regarding the retention, deletion, or return of Personal Data shall be governed by the terms of the Data Processing Agreement (DPA). In the event of any conflict between this Agreement and the DPA regarding data handling, the terms of the DPA shall prevail.

12.5 Survival

The obligations of confidentiality under this Agreement shall survive termination or expiration of this Agreement for a period of five (5) years.

Notwithstanding the foregoing:

(a) any obligations relating to Personal Data shall survive for so long as required under applicable Data Protection Laws and the Data Processing Agreement; and

(b) any trade secrets, source code, algorithms, security procedures, encryption methods, non-public technical architecture, proprietary models, or other information constituting a trade secret under applicable law shall remain confidential for so long as such information retains its status as a trade secret under applicable law.

13. TERMINATION AND SUSPENSION

13.1 Termination for Cause

Either party may terminate this Agreement immediately by giving written notice if the other party:

(a) Commits a material breach of this Agreement and:

(i) The breach is not remediable; or

(ii) The breach is remediable but is not cured within 30 days of written notice.

(b) Persistently breaches any terms of this Agreement, even if no single breach is considered material.

(c) Becomes subject to insolvency, liquidation, or administration proceedings.

13.2 Termination for Convenience

- The Customer may terminate this Agreement by providing written notice of termination at least:

  (a) 60 days before the end of the Subscription Term for Subscriptions longer than one month; or

  (b) 7 days before the end of the Subscription Term for rolling monthly Subscriptions.

- The Provider may terminate the Agreement providing at least 180 days' written notice.

13.3 Suspension of Services

The Provider may suspend access to the Platform immediately (without terminating the Agreement) if:

(a) The Customer fails to pay any amount due beyond 15 days.

(b) The Customer engages in fraudulent, illegal, or unauthorised activities.

(c) The Customer's use of the Platform poses a security risk or disrupts other users.

(d) Compliance with regulatory obligations requires suspension.

(e) The Provider must suspend services to comply with a court order or governmental request.

The Provider will notify the Customer of any suspension and will work in good faith to restore services upon resolution of the issue.

13.4 Effect of Termination

- Termination or expiration of this Agreement shall take effect in accordance with the applicable notice provisions of this Agreement. The consequences of termination, including cessation of access, data handling, migration assistance, payment obligations, and survival of rights and obligations, are governed by Clause 14 and the Data Processing Agreement.

14. EFFECTS OF TERMINATION

14.1 Consequences of Termination

Upon termination of this Agreement, all rights and obligations under this Agreement shall cease, except for:

- Clauses that explicitly survive termination, including but not limited to Clauses 1, 5, 7, 9, 10, 12, 14, 15, 17 and 18;
- Any accrued rights or liabilities of either party as of the termination date;
- The Customer's obligation to pay any outstanding fees due prior to termination.

14.2 Data Deletion & Retention

Upon termination or expiration of this Agreement, the Provider shall handle Customer Materials and Personal Data in accordance with the Data Processing Agreement, including applicable provisions relating to:

(a) retention periods;
(b) return or export of Customer Materials;
(c) deletion or anonymisation procedures;
(d) legal, regulatory, audit, backup, disaster recovery, and security retention obligations; and
(e) applicable post-termination access rights.

In the event of any conflict between this Agreement and the Data Processing Agreement regarding Personal Data processing, retention, deletion, export, or return obligations, the Data Processing Agreement shall prevail.

14.3 Post-Termination Assistance and Data Migration

Subject to payment of applicable Fees and the Customer's compliance with this Agreement, the Provider may provide reasonable post-termination assistance for a period of up to ninety (90) days following the effective date of termination or expiration of this Agreement ("Transition Period").

During the Transition Period, the Customer may submit written requests for:

(a) export of Customer Materials held within the production environment of the Platform in a commonly used machine-readable format reasonably determined by the Provider, which may include CSV, JSON, XLSX, PDF, or other standard industry formats;

(b) reasonable transition and migration assistance relating to the transfer of Customer Materials to another service provider or internal system; and

(c) administrative cooperation reasonably required to support orderly service transition activities.

Unless otherwise expressly agreed in writing:

(i) post-termination assistance, migration services, restoration work, custom export formatting, technical consultancy, and related services shall be charged at the Provider's then-current professional services rates;

(ii) the Provider is not responsible for:

- data transformation beyond standard export functionality;
- compatibility with third-party systems;
- migration validation;
- testing activities;
- rebuilding integrations; or
- errors introduced outside the Provider's systems following export;

(iii) the Customer remains solely responsible for:

- verifying exported data;
- completing migration activities;
- maintaining regulatory records; and
- ensuring continuity of its own regulated operations;

(iv) archived backups, disaster recovery systems, security backups, logs, telemetry, and residual retained data may not be immediately accessible, searchable, or exportable during the Transition Period and shall continue to be governed by the Data Processing Agreement and applicable retention policies;

(v) following expiration of the Transition Period, the Provider may delete or anonymise Customer Materials in accordance with this Agreement, the Data Processing Agreement, applicable law, and the Provider's standard retention procedures.

Nothing in this Clause obliges the Provider to retain Customer Materials beyond applicable retention periods or to provide bespoke transition services unless separately agreed in writing.

14.4 Customer's Responsibilities Upon Termination

1. **Cessation of Use:**
   Upon termination, the Customer shall:
   - Cease using and prevent further use of the Platform and Services;
   - Pay all outstanding fees due under this Agreement;
   - Return or destroy any Documentation provided by the Provider;
   - Ensure all Authorised Users cease accessing the Platform.
2. **Final Billing & Settlements:**
   The Provider may issue a final invoice for outstanding amounts due under this Agreement, payable within seven (7) days of issuance.

14.5 Suspension or Termination for Non-Payment

Where Services are suspended or terminated due to non-payment, the Provider may restrict access to the Platform, Customer Materials, support services, and export functionality until all undisputed overdue amounts and applicable restoration or recovery Fees are paid.

The Provider shall continue to protect retained Customer Materials in accordance with the Data Processing Agreement and applicable law during any applicable retention period.

15. NOTICES

15.1 Form of Notice

Any notice or communication given under this Agreement must be in writing and may be delivered:

(a) personally;
(b) by recognised courier or recorded delivery service;
(c) by email to the designated notice email address of the receiving party; or
(d) by electronic notification through the Platform for operational, service, support, renewal, billing, policy, security, or administrative notices.

Notices relating to termination, non-renewal, material breach, suspension, indemnity claims, changes to Fees, legal disputes, or other legal matters may validly be delivered by email.

15.2 Recipient Details

Unless otherwise updated in writing, notices shall be sent to:

The Provider
Nicholas Jordan (Director)
Nuworks Ltd
Suite 5, 26-27 West Street
Horsham, West Sussex, RH12 1PB
Email: nick.jordan@nuworks.com

The Customer
As per details on the Order Form (Order Form)

15.3 Receipt of Notices

A notice shall be deemed received:

(a) if delivered personally, at the time of delivery;

(b) if sent by courier or recorded delivery service, two (2) Business Days after dispatch;

(c) if sent by email, at the time of transmission, provided that the sending party does not receive an automated delivery failure or bounce notification within a reasonable period after transmission; and

(d) if delivered through the Platform, at the time the notice is made available to the Customer's designated administrative account or notification centre.

Where deemed receipt would occur outside Business Hours, receipt shall instead occur at the start of the next Business Day.

15.4 Address and Email Updates

- Each party must promptly notify the other in writing of any changes to its contact details for the purposes of notices under this Agreement. If the Customer fails to update its contact details, any notice sent to the last known address or email will be considered duly served.

15.5 Legal Notices and Indemnification Claims

- Notices relating to termination, non-renewal, material breach, indemnity claims, formal disputes, suspension, or other legal matters may be delivered using any method permitted under Clause 15.1.
- Nothing in this Clause prevents either party from serving court proceedings or formal legal process in any manner permitted by applicable law.

15.6 Application to Data Processing Agreement

Unless otherwise expressly stated in the Data Processing Agreement, all notices, communications, approvals, objections, requests, and other correspondence relating to the Data Processing Agreement shall be governed by this Clause 15.

16. FORCE MAJEURE

16.1 Suspension of Obligations

- Neither party shall be liable for any failure or delay in the performance of its obligations (excluding payment obligations) under this Agreement due to a Force Majeure Event. Such obligations shall be suspended for the duration of the Force Majeure Event.

16.2 Definition of Force Majeure Event

A **"Force Majeure Event"** means any event or circumstance beyond a party's reasonable control, including, but not limited to:

(a) Acts of God, natural disasters (such as earthquakes, floods, hurricanes, and wildfires), and extreme weather conditions;

(b) Acts of war, hostilities, terrorism, civil unrest, riots, strikes, industrial disputes, or government-imposed lockdowns;

(c) Failures, outages, or disruptions of the internet, telecommunications, power, or utility services that are beyond the reasonable control of the affected party;

(d) Cyberattacks, ransomware attacks, or malicious third-party cybersecurity incidents beyond the reasonable control of the affected party;

(e) Compliance with any law, government order, regulation, embargo, or trade restriction;

(f) Pandemics, epidemics, or other public health crises that prevent the party from fulfilling its obligations.

16.3 Notification and Mitigation

A party that is affected by a Force Majeure Event shall:

(a) Notify the other party as soon as reasonably practicable, specifying the nature and expected duration of the event; and

(b) Use commercially reasonable efforts to mitigate the impact of the Force Majeure Event and resume performance of its obligations as soon as reasonably possible.

16.4 Extended Force Majeure and Right to Terminate

- If the Force Majeure Event continues for more than 60 days, either party may terminate this Agreement by providing written notice to the other party. In such a case, no liability shall arise from such termination, except for any outstanding payments owed by the Customer for Services provided up to the termination date.

16.5 Exclusion of Payment Obligations

- The occurrence of a Force Majeure Event shall not relieve the Customer of its obligation to pay any Fees due under this Agreement unless explicitly agreed otherwise in writing by the Provider.

17. DISPUTE RESOLUTION

17.1 Good Faith Negotiations

In the event of any dispute, controversy, or claim arising out of or relating to this Agreement (including its formation, validity, performance, or termination), the parties shall first attempt in good faith to resolve the dispute through negotiations between authorised representatives of each party.

17.2 Continued Performance

Unless prohibited by law or where termination rights are exercised in accordance with this Agreement, each party shall continue to perform its obligations under this Agreement while any dispute is being resolved.

18. GENERAL

18.1 Waiver

- No failure or delay by either party in exercising any right, power, or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise of that right, power, or privilege. Any waiver of any breach of this Agreement must be in writing and signed by the waiving party.

18.2 Severability

- If any provision of this Agreement is determined by a court or other competent authority to be unlawful, invalid, or unenforceable, the remainder of the Agreement will remain in effect. If any invalid, illegal, or unenforceable provision would be valid, legal, and enforceable if modified, then such provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

18.3 Entire Agreement

(a) This Agreement, including any referenced schedules, exhibits, policies, or addenda, constitutes the entire agreement between the parties with respect to its subject matter and supersedes all prior agreements, understandings, or arrangements (whether written or oral) relating to the same subject matter.

(b) Neither party shall be entitled to rely on any statement, representation, warranty, or understanding other than as expressly set out in this Agreement.

18.4 Assignment

- Neither party may assign, transfer, delegate, or otherwise deal with its rights and obligations under this Agreement without the prior written consent of the other party, which shall not be unreasonably withheld. However, the Provider may assign this Agreement in the event of a corporate restructuring, sale, or transfer of business, provided that the assignee assumes all obligations under this Agreement.

18.5 No Third-Party Rights

- This Agreement is for the sole benefit of the parties and their permitted assigns, and nothing herein, express or implied, is intended to or shall confer any rights, benefits, or remedies of any nature whatsoever upon any third party. The Contracts (Rights of Third Parties) Act 1999 shall not apply to this Agreement.

18.6 Governing Law and Jurisdiction

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it, its subject matter, or formation shall be governed by and construed in accordance with the laws of England and Wales.

The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

Nothing in this Agreement shall prevent either party from seeking:

- interim, injunctive, or equitable relief in any court of competent jurisdiction;
- debt recovery proceedings; or
- enforcement of intellectual property rights or confidentiality obligations.

18.7 Changes to Incorporated Policies and Service Documents

(a) The Provider may update or modify the following documents from time to time:

(i) the Acceptable Use Policy (AUP);
(ii) Schedule 1 (Service Level Schedule);
(iii) the Privacy Policy;
(iv) operational policies, privacy controls, Tracking Technologies controls, cookie governance requirements, security requirements, support procedures, or technical documentation incorporated into this Agreement; and
(v) any Supplemental Terms applicable to optional features or third-party integrations,

provided that such changes are reasonably necessary for:

(A) compliance with applicable law, regulation, or security requirements;
(B) reflecting changes to the Platform, Services, or business operations;
(C) improving security, functionality, or customer experience; or
(D) preventing misuse, fraud, or operational risk.

(b) The Provider shall provide the Customer with at least thirty (30) days' prior notice of any material changes to the documents listed in Clause 18.7(a), including by email, electronic notification within the Platform, or publication on the Provider's website.

(c) Non-material changes, including administrative corrections, clarifications, formatting updates, or changes required by law, may take effect immediately upon notice.

(d) If a change under this Clause 18.7 materially and disproportionately adversely affects the Customer's use of the Services, and such change is not reasonably required for legal, regulatory, security, operational, technical, infrastructure, third-party dependency, or service improvement purposes, the Customer may elect not to renew the affected Services by providing written notice to the Provider before the commencement of the next renewal term.

(e) A non-renewal under Clause 18.7(d):

(i) shall take effect at the end of the then-current Subscription Term;
(ii) shall not affect the validity or enforceability of the revised terms during the current or renewed Subscription Term;
(iii) shall not relieve the Customer of payment obligations accrued prior to termination; and
(iv) shall be the Customer's sole and exclusive remedy in respect of such change.

(f) Continued access to or use of the Services after the effective date of a notified change constitutes acceptance of the revised documents.

(g) For the avoidance of doubt, material amendments to the Data Processing Agreement affecting:

(i) the allocation of liability;

(ii) data protection roles;

(iii) lawful processing obligations; or

(iv) international data transfer mechanisms,

shall require mutual written agreement between the parties unless such amendment is required by applicable law, regulatory guidance, court order, or a mandatory update to recognised transfer mechanisms including Standard Contractual Clauses or equivalent approved transfer mechanisms.

18.8 Amendments

Except as expressly permitted under Clause 18.7 (Changes to Incorporated Policies and Service Documents), no modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by duly authorised representatives of both parties.

18.9 Survival

- The provisions of this Agreement that by their nature should survive termination or expiration (including but not limited to confidentiality, data protection, indemnities, limitation of liability, and dispute resolution) shall remain in effect after the termination or expiration of this Agreement.

18.10 **Electronic Acceptance and Contract Formation**
By accessing, registering for, purchasing, electronically accepting, signing, installing, or using the Platform or Services, the Customer acknowledges and agrees that:

(a) electronic acceptance of this Agreement, including by click-through acceptance, electronic signature, account registration, execution through an approved e-signature platform, or continued use of the Services, constitutes valid and legally binding acceptance of this Agreement;

(b) the individual accepting this Agreement represents and warrants that they have the authority to bind the Customer and any relevant legal entity on whose behalf access to the Services is obtained;

(c) electronic records maintained by the Provider relating to acceptance of this Agreement, including timestamps, account credentials, acceptance logs, version records, IP addresses, user identifiers, device information, audit logs, and related electronic evidence, shall be admissible in evidence to the fullest extent permitted by applicable law and shall constitute prima facie evidence of execution, acceptance, and use of the Services; and

(d) the parties agree that this Agreement and any related notices, consents, approvals, records, or communications may be executed, delivered, retained, and evidenced electronically.

SCHEDULE 1 - SERVICE LEVEL

1. INTRODUCTION

1.1 Purpose

- This Service Level Schedule sets out general service availability and support provisions for the Platform.

1.2 Service Performance

- The Provider will use commercially reasonable efforts to maintain service performance as per this Schedule.

1.3 Scope

- This Schedule applies to:

    (a) The Platform and related services;

    (b) Customer-specific platform usage; and

    (c) Customer Data stored within the Platform.

1.4 Exclusions

- The Provider is not responsible for service disruptions caused by:

    (a) Customer-side network or device failures;

    (b) Third-party software or integrations; or

    (c) Unapproved modifications made by the Customer.

2. SUPPORT SERVICES

2.1 Availability

- The Provider shall make available support services as follows:
    - **Standard Support:** Available during Business Hours on Business Days.
    - Response times and resolution efforts will be handled on a commercially reasonable basis.

2.2 Logging Support Requests

- Support requests must be logged through the Helpdesk portal or designated communication channels.

2.3 Prioritisation

- The Provider reserves the right to prioritise support tickets based on urgency and business impact.

3. SERVICE AVAILABILITY

3.1 General Availability

- The Provider will use commercially reasonable efforts to ensure the availability of the Platform.

3.2 Target Availability

The Provider will use commercially reasonable efforts to maintain monthly Platform availability of 99.5%, excluding:

- scheduled maintenance;
- emergency maintenance;
- Force Majeure Events;
- third-party outages or dependencies outside the Provider's reasonable control;
- Customer-caused disruptions;
- issues caused by Customer systems, configurations, integrations, networks, devices, credentials, or third-party services;
- suspension, restriction, or unavailability arising from Customer breach, non-payment, security risk, misuse, or legal or regulatory requirements; and
- Beta Services, evaluation features, sandbox environments, test environments, or non-production functionality.

Availability targets are service objectives only and do not constitute warranties, guarantees, service level commitments, or remedies.

3.3 Interruptions

- Service interruptions may occur due to scheduled maintenance, third-party service provider failures, force majeure events, or other factors beyond the Provider's reasonable control.

4. SERVICE CREDITS

- The Provider does not provide service credits for any service interruptions or downtime.

5. SCHEDULED MAINTENANCE

5.1 Maintenance Windows

- The Provider may perform scheduled maintenance as needed and will endeavor to provide reasonable notice where possible.
- Scheduled maintenance will generally be performed outside normal UK business hours where reasonably practicable.

5.2 Urgent Maintenance

- Maintenance may be carried out without prior notice in urgent situations.

6. BACKUPS AND DATA RESTORATION

6.1 Backup Procedures

The Provider shall maintain commercially reasonable backup procedures designed to support the availability and restoration of Customer Data stored within the production environment of the Platform.

Backup procedures are operational resilience measures and do not constitute a guarantee that all Customer Data, historical versions, metadata, configurations, integrations, logs, telemetry, or system states will be recoverable.

Unless otherwise agreed in writing:

- backups may include a combination of snapshot, replication, incremental, differential, or full backup methodologies;
- backup frequency, retention periods, storage architecture, restoration approach, and replication methods may be determined and modified by the Provider from time to time based on operational, technical, security, resilience, infrastructure, and business requirements; and
- backup systems may include encrypted cloud-based, geographically redundant, or third-party managed infrastructure environments.

The Provider does not guarantee uninterrupted availability, zero data loss, recovery of all historical data versions, or restoration to any specific point in time.

6.2 Restoration Requests

The Customer may request restoration of Customer Data where data loss, corruption, deletion, or operational recovery circumstances reasonably require restoration activities.

The Provider shall use commercially reasonable efforts to restore the most recent reasonably available backup copy determined by the Provider to be operationally recoverable.

Restoration activities:

- are subject to system availability, technical feasibility, security requirements, data integrity considerations, legal and regulatory constraints, and operational capacity;
- may not restore all data, metadata, configurations, integrations, logs, telemetry, permissions, audit trails, or historical states;
- may require temporary service interruption, restricted system access, or other operational measures; and
- may be refused, limited, delayed, or modified where restoration would create security, legal, regulatory, operational, data integrity, or third-party dependency risks.

Unless restoration is required solely due to the Provider's breach of this Agreement or applicable Data Protection Laws, the Provider may charge reasonable Fees for:

- restoration requests;
- recovery investigations;
- historical retrieval requests;
- bespoke restoration work;
- customer-requested recovery testing;
- customer-requested export activities; and
- technical, operational, or professional services required to support restoration.

6.3 Recovery Objectives

Any recovery objectives, recovery time estimates, restoration priorities, backup frequency statements, retention statements, operational resilience targets, or disaster recovery targets communicated by the Provider are objectives only and do not constitute binding warranties, guarantees, service level commitments, RTOs, RPOs, or remedies.

The Provider does not provide binding Recovery Time Objective (RTO), Recovery Point Objective (RPO), disaster recovery testing, backup retention, or restoration commitments unless expressly stated in a separate written agreement signed by the Provider.

6.4 Retention and Archived Backups

Archived backups, disaster recovery copies, system redundancy environments, logs, telemetry, and residual retained data may continue to exist for operational, legal, regulatory, security, audit, resilience, backup, archive, or disaster recovery purposes following deletion requests or termination of the Agreement, subject to the Data Processing Agreement and applicable retention policies.

7. CUSTOMER RESPONSIBILITIES

The Customer must:

- Ensure staff are trained in Platform usage;
- Appoint a primary contact for support communications;
- Maintain a stable network connection;
- Use compatible third-party software integrations.

8. AMENDMENTS

8.1 Schedule Changes

- The Provider reserves the right to amend this Schedule with reasonable notice.

8.2 Material Reductions

- Amendments shall not materially reduce service commitments without mutual agreement.

SCHEDULE 2 - ADDITIONAL PROJECTS

1. INTRODUCTION

1.1 Definition of New Functionality

- **"New Functionality"** refers to a new module or a brand-new function within the Platform that introduces additional capabilities not previously available. New Functionality may be subject to separate charges, and will not be considered a standard upgrade. Requests for New Functionality shall be assessed through the Additional Projects Request Process and be subject to commercial agreement.

1.2 Scope of Additional Projects

- The Customer may request modifications or enhancements to the Services ("Additional Projects"). Additional Projects include, but are not limited to:

    (a) Amendments to Customer-specific Platform use requirements (as set out in the Order Form);

    (b) Modifications to Customer Materials;

    (c) Enhancements or modifications to the Platform (excluding general Upgrades or New Functionality);

    (d) Modifications to the sandbox environment.

1.3 Exclusions

The following are not considered Additional Projects under this Schedule:

(a) Modifications or enhancements classified as standard, as defined by the Provider;

(b) Routine updates, bug fixes, and maintenance performed as part of the Provider's general service commitments;

(c) Services already included within the Customer's existing licence agreement unless otherwise agreed as New Functionality;

(d) Any requests that fall outside the technical or operational scope of the Platform, as reasonably determined by the Provider.

2. ADDITIONAL PROJECTS REQUEST PROCESS

2.1 Submission

- All Additional Project requests must be submitted using the Additional Projects Request Form.

2.2 Evaluation

- The Provider is under no obligation to accept any Additional Project requests but will use commercially reasonable efforts to evaluate such requests.

2.3 Feasibility and Scoping

- If an Additional Project requires a feasibility assessment, cost estimation, and timeline determination ("Scoping"), both parties shall follow the structured process outlined in Section 5.

3. PROJECT WORK AND SCOPING

3.1 Project Work

- Approved Additional Projects will be delivered as Project Work under this Agreement.
- The scope, pricing, and implementation timeline will be agreed upon through the Additional Projects Request Form.

3.2 Scoping

- If required, the Provider shall conduct a Scoping Phase to assess feasibility, estimate costs, and determine timelines.
- Scoping shall only begin upon the Customer's written approval via Part 3(a) of the Additional Projects Request Form.

4. PAYMENT TERMS FOR ADDITIONAL PROJECTS

4.1 Scoping Fees

- Scoping shall not commence until the Customer has signed Part 3(a) of the Additional Projects Request Form.
- Scoping Charges must be paid within 10 days of:

  (a) Completion of Scoping, or

  (b) Issuance of an invoice—whichever is later (unless otherwise agreed in writing).

4.2 Project Work Fees

- Project Work shall not commence until the Customer has signed Part 3(b) of the Additional Projects Request Form.
- Charges must be paid within 10 days of:

  (a) The Provider confirming completion and making the Project Work available to the Customer in the live Platform or sandbox, or

  (b) Issuance of the appropriate invoice—whichever is later (unless otherwise agreed in writing).

4.3 Licence Charge Adjustments

- Any increase in Licence Fees arising from Additional Projects shall be proportionally applied and reflected in the Order Form.

5. ADDITIONAL PROJECTS REQUEST SUBMISSION

Requests for Additional Projects shall be submitted using a method determined by the Provider from time to time, which may include an online form, customer portal, email, ticketing system, or other agreed process.

The request process will typically capture, where applicable:

- the Customer's details and relevant Agreement or Order Form;
- a description of the requested Additional Project;
- any requested timescales or delivery requirements;
- whether a scoping exercise is required;
- any estimated costs, Fees, Licence Fee adjustments or other commercial terms;
- any estimated implementation timescales;
- the Customer's approval of any quotation, scope or commercial terms before work commences; and
- confirmation of completion or acceptance of the work, where applicable.

The Provider may amend or update the request process and the information required from time to time, provided such changes do not materially reduce the Customer's rights under this Agreement.

6. UPDATES TO THE AGREEMENT

6.1 Order Form (Order Form) Updates

- Upon completion of any Additional Project, the Order Form shall be updated (or deemed updated) to reflect changes to the Platform and/or Services.

6.2 Licence and Fee Adjustments

- Any changes impacting Licence Fees will be formally recorded in the Order Form.