
MANAGED SERVICES

ULTIMA IT GENERAL TERMS

Underpinning terms applicable to
all UltimaIT managed services

Version Control

v1.0.0

Publish Date

19/09/2026





Sections

1. AGREEMENT STRUCTURE, ORDERS, AND PRECEDENCE	4
2. COMMENCEMENT, DURATION AND RENEWAL	4
3. SUPPLIER OBLIGATIONS AND SERVICE DELIVERY	4
4. CUSTOMER PREREQUISITES AND RESPONSIBILITIES	5
5. SECURITY, PATCHING, AND CUSTOMER CHANGES	6
6. SCOPE CHANGES AND OUT-OF-SCOPE WORK	7
7. THIRD-PARTY PRODUCTS, SOFTWARE AND SERVICES	7
8. EQUIPMENT AND PHYSICAL GOODS	8
9. CHARGES, INVOICING, AND PAYMENT	8
10. CONFIDENTIALITY	9
11. DATA PROTECTION	9
12. INTELLECTUAL PROPERTY	10
13. BACKUPS, DATA RECOVERY, AND BUSINESS CONTINUITY	10
14. WARRANTIES AND EXCLUSIONS	10
15. LIMITATION OF LIABILITY	11
16. SUSPENSION	11
17. TERMINATION AND EARLY TERMINATION	11
18. EXIT ASSISTANCE AND OFFBOARDING	12
19. FORCE MAJEURE	12
20. NOTICES AND COMMUNICATIONS	12
21. ASSIGNMENT AND SUBCONTRACTING	12
22. DISPUTE ESCALATION	13
23. GENERAL PROVISIONS	13
24. GOVERNING LAW AND JURISDICTION	13
25. DEFINITIONS AND INTERPRETATIONS	14
25.1. GENERAL DEFINITIONS	14
25.2. TECHNICAL DEFINITIONS	15



Use of these terms

These General Terms are intended to form one part of a modular contractual framework. A customer normally signs the Proposal or Order, which expressly incorporates the applicable documents below.

Document	Purpose
Proposal / Order	Customer-specific commercial terms: Services, quantities, Charges, Minimum Term, billing and Service Commencement Date.
Service Definitions / Service Schedule	Operational scope, inclusions, exclusions, support hours, service targets and Customer responsibilities.
General Terms (this document)	Underpinning legal and commercial framework applying across Orders.



From herein, “**Customer**” is defined as the legal entity identified as the **customer** in the applicable **Order**. The “**Supplier**” is defined as **Ultima Media Services Limited** trading as **UltimaIT**, a registered company in England and Wales, registration number: 14672272. Registered office address: 71 Millbrook Drive, Havant, Hampshire, PO9 5JX.

1. Agreement structure, Orders, and precedence

- 1.1. These **General Terms** establish the framework under which the **Supplier** may provide **Services**, **Software** and **Equipment** to the **Customer**. **Customer**-specific commercial and technical details will be set out in an **Order** and the applicable **Service Definitions**.
- 1.2. An **Order** becomes binding when accepted in the manner stated in that **Order**, including by authorised signature or electronic signature. The **Supplier** may also expressly accept an **Order** in writing.
- 1.3. Unless an **Order** expressly states otherwise, each accepted **Order** forms part of the **Agreement** and does not create a separate set of general terms.
- 1.4. If documents conflict, the following **order** of precedence applies only to the extent of the conflict: (a) a signed **Change Order**; (b) the applicable **Order**; (c) any applicable **Data Processing Addendum** for data protection matters; (d) the applicable **Service Definitions**; and (e) these **General Terms**.
- 1.5. No purchase **order** or other **Customer** document will amend the **Agreement** merely because it is issued, referenced or accepted for administrative purposes, unless the **Supplier** expressly agrees to the amendment in writing.

2. Commencement, duration and renewal

- 2.1. The **Agreement** comes into effect when the first **Order** is accepted and continues while any **Order** remains active, unless terminated in accordance with the **Agreement**.
- 2.2. A recurring **Service** begins on its **Service Commencement Date**. Any **Minimum Term** runs from that date unless the **Order** states otherwise.
- 2.3. The renewal arrangement, notice period and any renewal term for a recurring **Service** will be stated in the applicable **Order**. If an **Order** is silent, the **Parties** should agree the renewal position in writing before **Service Commencement**.
- 2.4. Implementation, onboarding and target delivery dates are reasonable estimates unless an **Order** expressly identifies a date as a binding contractual milestone.

3. Supplier obligations and service delivery

- 3.1. The **Supplier** will perform the **Services** with reasonable skill and care and in material accordance with the applicable **Order** and **Service Definitions**.
- 3.2. Service hours, support channels, priorities and response or resolution targets apply only where expressly stated in the applicable **Service Definitions** or **Order**.
- 3.3. Unless expressly stated as a guaranteed service level, response and resolution times are operational targets and not warranties of a fixed resolution time.
- 3.4. SLAs apply solely to **Services** where explicit response, resolution, or availability metrics are defined in an applicable **Order** or SLA Schedule.

- 3.5. SLAs do not apply to service failures caused by **Customer** error, third-party vendor outages, unauthorised environment modifications, or events of Force Majeure.
- 3.6. The **Supplier** may use employees, contractors and subcontractors to deliver the **Services** and remains responsible for performance of its contractual obligations, subject to the **Agreement**.
- 3.7. Maintenance Windows: The **Supplier** reserves the right to perform scheduled maintenance, updates, and emergency security patching. The **Supplier** shall use reasonable endeavours to give advance notice for scheduled maintenance and conduct non-urgent maintenance outside standard business hours. Scheduled maintenance shall not constitute downtime under any SLA.

4. Customer prerequisites and responsibilities

- 4.1. The **Customer** will provide timely cooperation, accurate information, decisions, approvals and access reasonably required to deliver the **Services**
- 4.2. The **Customer** will provide or procure appropriate administrative access, credentials, remote access, site access, licences, permissions and third-party support entitlements required for the **Supplier** to manage the agreed **Customer Environment**.
- 4.3. The **Customer** is responsible for ensuring that its **Users** are authorised to receive the **Services** and comply with reasonable security and operational instructions issued by the **Supplier**.
- 4.4. The **Customer** will notify the **Supplier** promptly of starters, leavers, material device or infrastructure changes, suspected security incidents and other changes that may affect the **Services**.
- 4.5. The **Customer** will maintain a safe working environment for any **Supplier** personnel attending its premises and disclose known hazards before attendance.
- 4.6. The **Customer** confirms that information supplied to the **Supplier** in connection with the **Services** will, to the best of its knowledge, be complete and accurate. The **Supplier** is not responsible for delay or failure caused by materially inaccurate, incomplete or withheld information.
- 4.7. Onboarding and Environment Discovery: Quotations and **Orders** may be based on information supplied by the **Customer** or reasonably available to the **Supplier** before commencement of the **Services**. Onboarding, discovery or technical assessment may identify additional assets, Users, licences, dependencies, unsupported systems, security risks, configuration issues or other circumstances that were not reasonably apparent when the applicable **Order** was agreed.
- 4.8. Where such a discovery materially affects the scope, cost, risk or technical requirements of the **Services**, the **Supplier** will notify the **Customer** and may propose a **Change Order**, additional **Charges**, remediation work or reasonable changes to the applicable **Service** requirements.
- 4.9. The **Supplier** is not required to manage an undisclosed or newly discovered asset or assume responsibility for a material technical or security risk outside the agreed scope until any necessary change to the **Services** has been agreed.
- 4.10. Where a discovered condition creates an immediate and material risk to the security, stability or integrity of the **Customer Environment** or the **Supplier's** systems, the **Supplier** may take reasonable protective action in accordance with Sections 5 and 16.

5. Security, patching, and customer changes

- 5.1. The **Customer** must not intentionally disable, remove, bypass or materially interfere with security, monitoring, backup or management controls deployed as part of the **Services** without the **Supplier's** prior agreement, except where necessary to respond to an immediate emergency.
- 5.2. The **Supplier** is not responsible to the extent a failure, security incident or degradation results from unauthorised changes made by the **Customer**, a **User** or an unapproved third party, or from the **Customer** preventing the **Supplier** from carrying out agreed management activities.
- 5.3. Where the **Supplier** makes a material security or lifecycle recommendation in writing and the **Customer** elects not to implement it, the **Supplier** may record the risk and, where reasonably necessary, vary or suspend the affected **Service** until the risk is addressed.
- 5.4. Patching may affect application compatibility or performance. The **Supplier** may defer, withhold, remove or alter deployment of a patch where it reasonably considers this necessary to protect stability, security or compatibility, and may recommend vendor remediation or an upgrade.
- 5.5. Customer Environment Integrity: The **Customer** is solely responsible for ensuring its underlying network, internet connectivity, power infrastructure, and internal environment comply with the minimum specifications required by the **Supplier**.
- 5.6. The **Supplier** accepts no liability for service degradation where the customer has failed to maintain appropriate environmental conditions for the goods or services to be consumed within their working environment. In this event, the **Supplier** will remove any obligations to honour the SLAs as set out in the **Order**.
- 5.7. User Security Hygiene: The **Customer** shall maintain appropriate password policies, enable multi-factor authentication (**MFA**) for user accounts where supported and reasonably applicable, and ensure credentials and access rights for departed staff are revoked promptly. The **Customer** is responsible for activity carried out using its **User** credentials except to the extent resulting from the **Supplier's** breach of its obligations under the **Agreement**.
- 5.8. Unsupported and End-of-Life Technology: Where any hardware, **Software**, operating system, application, firmware or **Third-Party Service** within the **Customer Environment** becomes Unsupported or End-of-Life, the **Supplier** may notify the **Customer** and recommend replacement, upgrade, remediation or other reasonable action.
- 5.9. The **Supplier** may continue to provide **Services** in relation to **Unsupported** or **End-of-Life** technology where it reasonably considers it practicable and safe to do so, but does not warrant that such technology can be maintained, secured, patched, restored or made compatible with supported systems.
- 5.10. Where **Unsupported** or **End-of-Life** technology materially increases the security, operational or support risk associated with a **Service**, the **Supplier** may reasonably:
 - 5.10.1. exclude the affected technology from applicable SLAs or service targets;
 - 5.10.2. restrict or vary the scope of support provided in relation to the affected technology;
 - 5.10.3. require reasonable remediation, replacement or upgrade as a condition of continued support; or
 - 5.10.4. suspend or cease management of the affected technology where continued management would create a material security, operational or compliance risk.
- 5.11. The **Supplier** will give the **Customer** reasonable written notice before restricting, varying, suspending or ceasing a **Service** under Section 5.10, except where immediate action is reasonably necessary to protect the security or integrity of systems, networks or data.
- 5.12. The **Supplier** will not be responsible for failure, degradation, incompatibility, security vulnerabilities or other loss to the extent caused by the continued use of **Unsupported** or **End-of-Life** technology, except to the extent caused by the **Supplier's** breach of its obligations under the **Agreement**.

6. Scope changes and out-of-scope work

- 6.1. The **Services** are limited to the scope, quantities and supported assets stated in the applicable **Order** and **Service Definitions**.
- 6.2. Additional users, devices, servers, locations, licences, project work, major changes or other services outside the agreed scope may result in additional **Charges**.
- 6.3. Changes in Service Quantities: Where Charges are based on the number of Users, Managed Devices, Servers, Network Devices, licences, locations or other measurable units, the Customer will notify the Supplier promptly of any increase or decrease affecting the contracted quantity.
- 6.4. Additional units brought within the scope of a Service may be charged from the date on which the relevant unit is provisioned, licensed, onboarded or otherwise receives the benefit of the Service. Reductions will take effect from the next applicable billing period, subject to any Minimum Term, notice period or third-party commitment applicable to the affected unit.
- 6.5. Routine changes in quantities within the existing scope of a Service do not require a formal Change Order unless the applicable Order states otherwise. A material change to the nature or overall scope of the Services remains subject to the Change Order provisions of this Agreement.
- 6.6. Either **Party** may propose a **Change Order**. A material change to scope, **Charges**, **Minimum Term** or contractual commitments is effective only when agreed in writing by authorised representatives of both **Parties**.
- 6.7. Where immediate action is reasonably necessary to contain a serious security threat or prevent material service damage, the **Supplier** may take proportionate emergency action and notify the **Customer** as soon as reasonably practicable. Chargeable emergency work outside scope should be agreed where circumstances permit.
- 6.8. Authorisation of Out-of-Scope Work: Where the Customer requests work that falls outside the scope of the applicable Services, the Supplier will notify the Customer where reasonably practicable that the work may be subject to additional Charges before commencing it.
- 6.9. Chargeable work may be authorised by an Authorised Representative through an accepted quotation, Change Order, email, support Ticket or other agreed written communication. Such approval constitutes authority for the Supplier to perform and charge for the approved work.
- 6.10. The Customer is responsible for identifying those Users or representatives authorised to approve chargeable work. Unless the Supplier has been notified otherwise in writing, the Supplier may reasonably rely on approval given by an Authorised Representative or other Customer contact who has been presented to the Supplier as having authority to approve the relevant work.
- 6.11. Nothing in this Section prevents the Supplier from taking proportionate emergency action in accordance with Section 6.7 where prior approval cannot reasonably be obtained.

7. Third-party products, Software and Services

- 7.1. **Third-Party Services** and **Software** are subject to the relevant vendor's terms, licence conditions, technical limitations and service availability. The **Customer** agrees to comply with applicable end-user or **customer** terms notified to it.
- 7.2. The **Supplier** will use reasonable efforts to administer and support **Third-Party Services** included within scope but does not control, and does not warrant, the uninterrupted operation of third-party platforms, telecommunications services or vendor infrastructure.
- 7.3. Manufacturer or vendor warranties apply to third-party products where available. Unless expressly stated otherwise, the **Supplier** does not provide a separate manufacturer-equivalent warranty.

- 7.4. Where such a change results in a material increase to the **Charges** for an affected **Service**, the **Supplier** will give as much advance written notice as is reasonably practicable, having regard to the notice provided by the relevant third-party vendor. Any right to terminate the affected **Service** will remain subject to unavoidable third-party commitments already incurred.
- 7.5. Third-Party Commitments: Where the **Customer** requests or accepts a **Third-Party Service**, **Software** licence or subscription that requires the **Supplier** to enter into a fixed-term, minimum-term or non-cancellable commitment with a third-party vendor, distributor or provider, the **Customer** remains responsible for the **Charges** associated with that commitment for its remaining term, notwithstanding termination or reduction of the corresponding Service, except where termination results directly from the Supplier's uncured material breach.
- 7.6. The **Supplier** will, where reasonably practicable, identify any material minimum commitment applicable to a **Third-Party Service** within the applicable Order. The **Customer** acknowledges that third-party cancellation, reduction and renewal rights may be determined by the relevant vendor's terms and may differ from the termination rights applicable to the **Supplier's** own **Services**.

8. Equipment and physical goods

- 8.1. Equipment pricing, delivery, installation and payment terms will be stated in the applicable **Order** or quotation.
- 8.2. Risk of loss or damage to **Equipment** passes to the **Customer** on delivery to the agreed location, except to the extent caused by the **Supplier** before completion of any agreed installation work.
- 8.3. Retention of Title: Title to physical **Goods** purchased outright remains with the **Supplier** until the **Supplier** receives full cleared payment of the relevant invoice.
- 8.4. Instalment Purchases: Where payment for **Goods** is structured in instalments, legal title does not pass until the final instalment is cleared into the Supplier's bank account.
- 8.5. Software & SaaS: Title to **Software**, licenses, or "as-a-Service" platforms provided under this Agreement never passes to the **Customer**.
- 8.6. The **Supplier** will pass through the benefit of available manufacturer warranties where reasonably possible. Warranty claims remain subject to manufacturer terms and processes.
- 8.7. Delivery dates for **Equipment** are estimates unless expressly guaranteed. The **Supplier** is not responsible for delays caused by manufacturer, distributor or supply-chain events outside its reasonable control.

9. Charges, invoicing, and payment

- 9.1. The **Customer** will pay the **Charges** stated in each **Order** in pounds sterling unless otherwise agreed.
- 9.2. Unless an **Order** states otherwise: (a) recurring managed service and licence **Charges** are invoiced in advance; (b) variable consumption and time-and-materials **Charges** are invoiced in arrears; and (c) Equipment, one-off licences and project **Charges** are invoiced at the stage stated in the relevant **Order** or quotation.
- 9.3. Invoices are payable within 14 calendar days of the invoice date, unless the **Order** states a different payment period, via Direct Debit or electronic bank transfer.
- 9.4. The **Customer** must notify the **Supplier** promptly and in good faith of a disputed invoice, identifying the amount and reason for dispute. Undisputed amounts remain payable by the due date. Disputes should be raised to the Supplier within 10 business days of receipt.

- 9.5. Overdue undisputed sums may accrue statutory interest and compensation available under the Late Payment of Commercial Debts (Interest) Act 1998, together with reasonable recovery costs where permitted by law.
- 9.6. If an undisputed invoice remains materially overdue after written notice, the **Supplier** may suspend affected **Services** where reasonable and proportionate until payment is made. Suspension does not waive amounts properly due.
- 9.7. **Charges** are stated exclusive of VAT unless an **Order** states otherwise. While the **Supplier** is not VAT registered, VAT will not be charged. If the **Supplier** becomes required to charge VAT, applicable VAT will be added from the date required by law.
- 9.8. Changes to Recurring Charges: Unless an **Order** states otherwise, the **Supplier** may review and increase recurring **Charges** no more than once in any 12-month period by giving the **Customer** at least 30 days' written notice. Any increase will take effect on the date stated in that notice and will be reasonable having regard to increases in the **Supplier's** costs of providing the **Services**.
- 9.9. Section 9.8 does not restrict the **Supplier's** right to pass through changes in third-party costs, licensing, taxation or other charges in accordance with Section 7.4.

10. Confidentiality

- 10.1. Each **Party** will keep the other **Party's** Confidential Information confidential, protect it using at least reasonable care and use it only to perform or receive the **Services** or exercise rights under the **Agreement**.
- 10.2. Confidential Information may be disclosed to personnel, professional advisers, insurers, contractors and subcontractors who reasonably need it and are subject to appropriate confidentiality obligations, or where disclosure is required by law.
- 10.3. These obligations do not apply to information that is lawfully public, was already lawfully known without restriction, is independently developed, or is lawfully received from another source without a duty of confidence.
- 10.4. On termination, each **Party** will return or securely destroy the other **Party's** Confidential Information where reasonably requested, subject to legal, regulatory, insurance, backup and legitimate record-retention requirements.

11. Data protection

- 11.1. Each **Party** will comply with applicable UK data protection legislation in connection with the **Agreement**.
- 11.2. For ordinary account, billing and business-contact information, each **Party** may act as an independent controller for its own legitimate business administration purposes.
- 11.3. Where the **Supplier** Processes Personal Data on behalf of the **Customer**, the **Customer** will act as controller and the **Supplier** as processor unless the circumstances require a different lawful role allocation.
- 11.4. Detailed processor obligations, including documented instructions, confidentiality, security, subprocessors, international transfers, data-subject assistance, breach notification, audit information and deletion/return of Personal Data, should be set out in an applicable Data Processing Addendum.
- 11.5. The **Customer** is responsible for ensuring that it has an appropriate lawful basis, authority and transparency notices for Personal Data it instructs the **Supplier** to Process.

12. Intellectual property

- 12.1.** Each **Party** retains ownership of Intellectual Property Rights it owned or developed independently of the **Agreement**.
- 12.2.** The **Customer** retains ownership of **Customer Data** and **Customer** materials.
- 12.3.** The **Supplier** retains ownership of its pre-existing and reusable tools, scripts, templates, processes, methodologies, configurations, documentation frameworks and know-how, including improvements made while delivering the **Services**.
- 12.4.** Where the **Supplier** creates a **Customer**-specific Deliverable and an **Order** does not state different ownership terms, the **Supplier** grants the **Customer**, once applicable **Charges** are paid, a non-exclusive licence to use that Deliverable for its internal business purposes.
- 12.5.** Third-party **Software** and intellectual property remain subject to the relevant third-party licence terms.

13. Backups, data recovery, and business continuity

- 13.1.** Backup, disaster recovery and business continuity services are included only where expressly identified in an **Order** and **Service Definitions**.
- 13.2.** The existence of a managed IT or security service does not by itself mean that all **Customer Data** is backed up or recoverable.
- 13.3.** Where backup is included, restoration remains subject to successful backup jobs, configured scope and retention, source-system behaviour and the capabilities of the relevant backup platform. No backup system can guarantee recovery in every circumstance.
- 13.4.** Where no backup service is included for a workload, the **Customer** remains responsible for ensuring that it has an appropriate backup and recovery arrangement for that workload.

14. Warranties and exclusions

- 14.1.** Each **Party** warrants that it has authority to enter into and perform the **Agreement**.
- 14.2.** Except for express commitments in the **Agreement**, and to the extent permitted by law, the **Supplier** does not warrant that **Services** will be uninterrupted or error-free, that every security threat will be prevented or detected, or that third-party products will always remain available or compatible.
- 14.3.** The **Supplier** is not responsible for failures caused by unsupported or end-of-life systems, third-party outages, **Customer** or User acts or omissions, unauthorised changes, unavailable access, internet or utility failures, or other matters outside its reasonable control, except to the extent the **Supplier** has expressly accepted responsibility for the relevant matter.

15. Limitation of liability

- 15.1. Unrestricted Liability.** Nothing in the **Agreement** excludes or limits liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, or any other liability that cannot lawfully be excluded or limited.
- 15.2. Excluded Categories of Loss:** Subject to Section 15.1, the **Supplier** shall under no circumstances be liable to the **Customer** (whether in contract, tort (including negligence), breach of statutory duty, or otherwise) for:
- 15.2.1.** Loss of actual or anticipated profits;
 - 15.2.2.** Loss of sales, business, or revenue;
 - 15.2.3.** Loss of goodwill or commercial reputation;
 - 15.2.4.** Loss, damage, or corruption of data;
 - 15.2.5.** Indirect, special, or consequential loss.
- 15.3. Aggregate Liability Cap:** Subject to Sections 15.1 and 15.2, the **Supplier's** total aggregate financial liability arising under or in connection with this Agreement in any 12-month contract period shall be limited to 100% of the total Annual Charges paid or payable by the Customer under the specific Order giving rise to the claim during that 12-month period.
- 15.4. Cyber Attack Cap Sub-Limit:** Without prejudice to Section 15.3, the **Supplier's** total aggregate liability for loss arising from a malware infection, ransomware incident, or unauthorized network intrusion—where the Supplier has complied with its agreed security obligations—shall be strictly capped at the total fees paid under the affected **Order** over the preceding 6 months.
- 15.5.** Each **Party** will take reasonable steps to mitigate losses arising from a breach of the **Agreement**.

16. Suspension

- 16.1.** The **Supplier** may suspend all or part of an affected **Service** where reasonably necessary to: (a) protect the security or integrity of systems or data; (b) comply with **Applicable Law**; (c) respond to a serious **Customer** breach that prevents safe delivery; or (d) address materially overdue undisputed **Charges** after reasonable written notice.
- 16.2.** The **Supplier** will, where reasonably practicable, give advance notice, limit suspension to what is proportionate and restore the Service when the reason for suspension has been resolved.

17. Termination and early termination

- 17.1.** Either **Party** may terminate an affected **Order** for material breach if the other **Party** fails to remedy a remediable material breach within 30 days after receiving written notice identifying the breach. A **Party** may terminate immediately where a material breach is incapable of remedy.
- 17.2.** Either **Party** may terminate if the other becomes insolvent, enters administration or liquidation, ceases trading or is otherwise subject to an equivalent insolvency event, subject to Applicable Law.
- 17.3.** Termination for convenience may not take effect before expiry of an applicable **Minimum Term** unless the **Order** expressly permits it or the Parties agree an early termination arrangement.
- 17.4.** Upon termination of this **Agreement** or any **Order**:
- 17.4.1.** The **Customer** shall immediately pay all outstanding invoices and unbilled **Services** rendered up to the effective date of termination.
 - 17.4.2.** The **Customer** shall return all **Supplier**-owned hardware, equipment, software, and tools in its possession.
 - 17.4.3.** The **Supplier** shall revoke access to managed software licenses and tenant environments.

17.5. Termination does not affect rights, payment obligations or liabilities accrued before termination.

18. Exit assistance and offboarding

18.1. Following termination, and subject to payment of undisputed amounts due, the **Supplier** will provide reasonable cooperation to transition the **Customer** to its internal team or a replacement provider.

18.2. The **Supplier** will make available **Customer**-owned credentials and documentation held by it that are reasonably required for transition, subject to appropriate security verification.

18.3. Routine handover expressly included in a Service will be provided as stated in the **Service Definitions**. Material migration, data export, project work, extended consultancy or work requested by a replacement provider may be chargeable at the **Supplier's** then-current rates if agreed in advance.

18.4. **Supplier**-provided management agents, licences, access and tooling may be removed or revoked at the end of the applicable Service. The **Supplier** will not deliberately withhold **Customer**-owned credentials as leverage for disputed sums.

18.5. Any **Customer Data** retained by the **Supplier** after termination will be handled in accordance with the applicable Data Processing Addendum, retention requirements and agreed exit arrangements.

19. Force majeure

19.1. Neither **Party** is liable for delay or failure to perform an obligation, other than payment obligations already due, to the extent caused by an event beyond its reasonable control, including major utility or telecommunications failure, widespread third-party cloud disruption, natural disaster, government action, industrial action or similar event.

19.2. The affected **Party** will notify the other where reasonably practicable, take reasonable steps to mitigate the effect and resume performance as soon as reasonably possible.

19.3. Where a force majeure event prevents material performance of an affected Service for more than 60 consecutive days, either **Party** may terminate that affected **Service** on written notice, subject to unavoidable third-party commitments.

20. Notices and communications

20.1. Routine operational communications may be sent through the service desk, email or other agreed channels.

20.2. Formal notices relating to breach, termination or legal rights must be in writing and sent to the registered office and/or nominated contract email address stated in the **Order**.

21. Assignment and subcontracting

21.1. Neither **Party** may assign the **Agreement** or an **Order** without the other **Party's** prior written consent, not to be unreasonably withheld or delayed, except that the **Supplier** may assign to a successor acquiring substantially all the relevant business on written notice.

21.2. The **Supplier** may subcontract elements of the **Services**, including to specialist technology and cloud providers, while remaining responsible for its contractual obligations to the **Customer**, subject to applicable data protection requirements.

22. Dispute escalation

- 22.1.** Before commencing court proceedings, the **Parties** will use reasonable efforts to resolve a dispute through their nominated operational contacts and, if unresolved, escalate it to senior representatives.
- 22.2.** Nothing in this clause prevents either **Party** from seeking urgent interim relief, pursuing undisputed debt, preserving limitation rights or taking other action where delay would materially prejudice its rights.

23. General provisions

- 23.1.** Entire agreement. The **Agreement** constitutes the agreement between the **Parties** concerning its subject matter and supersedes prior discussions or representations on that subject, except for fraud or fraudulent misrepresentation.
- 23.2.** Variation and Updates to **General Terms**. The **Supplier** may update these **General Terms** from time to time to reflect changes in Applicable Law, regulatory requirements, technology, security requirements, industry practice, the **Supplier's** operating procedures or the manner in which the **Services** are provided.
- 23.2.1.** The **Supplier** will give the **Customer** reasonable written notice of any material change to these **General Terms**. Updated **General Terms** will take effect on the date specified in that notice and will apply to **Services** provided from that date.
- 23.2.2.** An update to these **General Terms** will not materially reduce the **Customer's** contracted **Services**, materially increase the **Customer's Charges**, or materially alter the **Customer's** rights or obligations during an existing **Minimum Term** unless the change is required by Applicable Law, results from a change imposed by a third-party provider, is otherwise expressly permitted by the **Agreement**, or is agreed between the **Parties** in writing.
- 23.2.3.** **Changes** to an **Order**, including material changes to scope, **Charges** or **Minimum Term**, remain subject to the applicable **Change Order** or other variation provisions of this **Agreement**.
- 23.2.4.** The version of the **General Terms** applicable from time to time will be identified by its version number and publication date.
- 23.3.** Severability. If a provision is invalid or unenforceable, it will be modified to the minimum extent necessary where lawful, or severed, without affecting the remaining provisions.
- 23.4.** Waiver. A failure or delay to exercise a right is not a waiver of that right. Any waiver must be in writing and applies only to the circumstances for which it is given.
- 23.5.** Third-party rights. Unless expressly stated otherwise, a person who is not a **Party** has no right to enforce the **Agreement** under the **Contracts (Rights of Third Parties) Act 1999**.
- 23.6.** Counterparts and electronic signature. **Orders** and other documents may be executed in counterparts and by electronic signature, with each executed counterpart forming part of the same agreement.
- 23.7.** Survival. Provisions intended by their nature to continue after termination, including confidentiality, accrued payment obligations, intellectual property, data protection, liability and exit provisions, will survive termination.

24. Governing law and jurisdiction

- 24.1.** This **Agreement**, and any dispute or claim arising out of or in connection with it or its subject matter (including non-contractual disputes), shall be governed by and construed in accordance with the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction to settle any such dispute or claim.

25. Definitions and Interpretation

This section sets out the definition of commonly used words and phrases applicable to both general and technical definitions.

25.1. General Definitions

Term	Definition
Agreement	This general commercial framework agreement , including all attached schedules, Service Level Agreements (SLAs), Data Processing Addenda (DPA), and accepted Orders .
Authorised Representative	An employee or designated agent of a party with express authority to bind that party to Orders or Agreement amendments.
Charges	The fees, prices, and recurring rates payable by the Customer for the supply of Goods, Software , or IT Services as outlined in an Order or Commercial Schedule.
Commercial Terms	The formal description of the prices, volumes, service definitions , service levels, delivery schedules, co-termination dates, cancellation terms, and permissible flexion of volumes deliverable by the Supplier .
Confidential Information	All proprietary, technical, commercial, or financial information relating to the business, affairs, customers , networks, or trade secrets of a party disclosed under this Agreement .
Customer Environment	The hardware, software , network infrastructure, cloud environments, and facilities managed, operated, or used by the Customer .
Customer Data	All electronic data, files, text, images, or personal data transmitted, stored, or processed by the Supplier on behalf of the Customer .
Deliverables	The hardware, software , configurations, documentation, or technical outputs created or delivered by the Supplier under an Order .
Force Majeure Event	Any event or circumstance beyond a party's reasonable control, including natural disasters, acts of government, warfare, terrorism, cyberattacks exceeding standard industry safeguards, major utility/telecommunications failures, or widespread third-party cloud service disruptions.
Goods	Physical hardware, equipment, servers, network hardware, or cabling provided to the Customer .
Intellectual Property Rights (IPR)	Patents, rights to inventions, copyright and related rights, trademarks, trade names, domain names, rights in get-up, goodwill, rights in designs, rights in computer software , database rights, and confidential information.
Minimum Term	The minimum contractual period for which a recurring Service is committed, as specified in the applicable Order .
Order	A proposal, quotation, order form, Statement of Work (SOW), Commercial Schedule or other document describing Goods or Services to be supplied under this Agreement , which is issued by the Supplier and accepted by the Customer in writing, or otherwise agreed in writing between the Parties.
Services	The IT managed services , cloud hosting, support, consultancy, security monitoring, or professional services supplied by the Supplier under an Order .
Service Commencement Date	The date on which a Service commences, as specified in the applicable Order , and from which any applicable Minimum Term and recurring Charges will apply unless otherwise stated.
Service Level Agreement (SLA)	The specific performance metrics, response times, uptime targets, and availability standards applicable to designated Services as set out in an Order or Service Schedule.
Software	Proprietary software tools, scripts, management platforms, or third-party software provided by or resold through the Supplier .

Third-Party Services / Software

Hardware, **software**, licenses, cloud subscriptions, or **services** owned and operated by third-**party** vendors (e.g., Microsoft, AWS, Cisco, Datto) and resold or managed by the **Supplier**.

25.2. Technical Definitions

Term	Definition
Backup	A separately retained copy of supported data or systems created for recovery purposes. The existence of a Backup does not guarantee that every item of data can be successfully restored.
BCDR – Backup and Disaster Recovery	A service providing backup and recovery capabilities intended to support restoration of systems, applications or data following failure, data loss or a disaster. BCDR may include image-based backups, replication or recovery infrastructure where specified in an Order .
Business Day	A day other than Saturday, Sunday or a public holiday in England.
Business Hours	The Supplier's normal support hours as stated in the applicable Service Definition or Order , excluding applicable public holidays unless otherwise stated.
Change / Request for Change (RFC)	A request to add, remove or modify a component, configuration or functionality within the Customer Environment or the scope of a Service.
Cloud Backup	A service that creates and retains copies of supported cloud-hosted Customer Data for restoration purposes in accordance with the applicable Service Definition, retention policy and capabilities of the relevant backup platform.
Device Hardening	The application of security configurations intended to reduce the attack surface and security risk of a supported device, including restricting unnecessary functionality and applying security policies.
DNS – Domain Name System	The distributed system used to translate domain names into IP addresses and provide other records required for internet and application services .
DNS Management	Administration of supported DNS zones and records on behalf of the Customer , as defined within the applicable Service Definition.

EDR – Endpoint Detection and Response	A cybersecurity technology used to monitor endpoint activity, detect potentially malicious behaviour and provide automated or administrator-initiated investigation, containment and remediation capabilities. EDR does not, by itself, constitute a 24/7 human-operated security monitoring service.
Endpoint	A supported end-user computing device connected to or accessing the Customer Environment , including a desktop computer, laptop or other device expressly identified within an Order or Service Schedule.
Entra ID	Microsoft's cloud-based identity and access management service, formerly known as Azure Active Directory.
Firewall	A physical or virtual security device or service that controls network traffic according to configured security and routing policies.
Hypervisor	Software or an operating-system role used to create, operate and manage Virtual Machines, including technologies such as Microsoft Hyper-V.
Incident	An unplanned interruption to, degradation of, or failure affecting a supported Service, Managed Device or component of the Customer Environment .
Intune	Microsoft's cloud-based endpoint management service used to manage supported devices, applications, configurations and security policies.
Major Change	A Change which, in the Supplier's reasonable assessment, presents material technical risk, requires substantial planning or engineering effort, or materially alters the Customer Environment and may therefore constitute chargeable project work.
Malware	Malicious software or code designed to disrupt, damage, access or otherwise interfere with systems, networks or data, including viruses, trojans, ransomware and similar threats.
Managed Device	An Endpoint, Server, network device or other supported asset that has been expressly included within the scope of a Managed Service.
Managed Endpoint	An Endpoint expressly included within the scope of the Supplier's Desktop Managed Service or another applicable Managed Service.

MDM – Mobile Device Management	Technology used to remotely enrol, configure, secure and manage supported devices.
MDR – Managed Detection and Response	A managed cybersecurity service combining security technology with ongoing human-led monitoring, investigation and response to detected threats, typically delivered by a Security Operations Centre or specialist security provider.
MFA – Multi-Factor Authentication	An authentication method requiring a User to provide two or more verification factors before access to an account, application or system is granted.
Microsoft 365 / M365	Microsoft's cloud productivity and collaboration platform, including services that may include Exchange Online, SharePoint Online, OneDrive, Teams, Entra ID and associated applications, subject to the Customer's applicable Microsoft licences.
Network Device	A physical or virtual device providing network functionality, including firewalls, routers, switches, wireless access points and other network infrastructure.
NMS – Network Monitoring and Management	The monitoring, administration and maintenance of supported Network Devices using remote management platforms and other Supplier tools.
Offboarding	The activities associated with ending or transitioning a Service, including removal of Supplier tooling, transfer of Customer -controlled information or credentials and reasonable cooperation with a replacement supplier .
Onboarding	The activities reasonably required to transition the Customer into a Managed Service, which may include discovery, documentation, deployment of Supplier tooling, configuration and establishment of administrative access.
Out-of-Scope Work	Work that is not expressly included within the applicable Order , Service Definition or Managed Service and which may be subject to additional Charges .
Patch	A software or firmware update intended to correct defects, improve functionality or address security vulnerabilities.
Patch Management	The controlled identification, assessment, deployment and monitoring of applicable software , operating-system or firmware updates to supported Managed Devices.

Project Services / Professional Services	Planned technical, consultancy, implementation, migration or other work provided outside the recurring scope of a Managed Service and normally subject to a separate quotation, Order or Statement of Work.
PSA – Professional Services Automation	The Supplier's business-management platform used for functions such as service desk tickets, customer records, service delivery, time recording, contracts and billing.
Ransomware	Malware designed to deny access to systems or data, commonly through encryption, and which may demand payment or another action in exchange for restoration or non-disclosure.
RDS – Remote Desktop Services	Microsoft Windows Server functionality allowing authorised Users to access applications or desktop sessions hosted on a Server remotely.
Resolution	The restoration of a Service to normal operation, or implementation of an acceptable workaround, such that the relevant Incident no longer materially prevents the affected functionality from being used.
Response Time	The period between an Incident or Service Request being accepted by the Service Desk and the Supplier commencing acknowledgement, triage or substantive investigation, as defined by the applicable SLA.
Restore / Restoration	The process of retrieving supported data, files, systems or workloads from an available Backup.
RMM – Remote Monitoring and Management	Software and associated services used by the Supplier to remotely monitor, manage, maintain and support Customer Devices, including collecting device health information, deploying configurations, executing administrative actions and managing software or operating system updates.
RPO – Recovery Point Objective	The target maximum period of data loss measured backwards from a disruptive event; for example, an RPO of four hours means the recovery design aims to make a recovery point no more than approximately four hours old.
RTO – Recovery Time Objective	The target period within which a service, system or workload is intended to be restored following a qualifying disruption. An RTO is a target unless expressly stated otherwise in an applicable SLA.
SaaS – Software as a Service	Software hosted and operated by a third-party provider and made available to Users over a network, normally on a subscription basis.

Security Alert	A notification generated by a security product or monitoring platform indicating activity that may require automated or human investigation. A Security Alert does not necessarily indicate that a Security Incident has occurred.
Security Baseline	A defined collection of security configurations and controls applied to supported systems or devices in accordance with an applicable Service Definition.
Security Incident	An actual or reasonably suspected event that compromises, or may compromise, the confidentiality, integrity or availability of systems, accounts, networks or data.
Server	A physical or virtual server operating-system instance identified as being within the scope of a Managed Service. Unless expressly stated otherwise, each separately managed operating-system instance constitutes one Server for charging and service-scope purposes.
Service Desk	The Supplier's function through which authorised Users may report Incidents, submit Service Requests and communicate with the Supplier regarding supported Services .
Service Request	A request from an authorised User for information, assistance, access, configuration or another standard activity that is not primarily the result of an Incident.
SLA – Service Level Agreement	The service performance measures expressly specified for a Service, which may include response, availability or other targets. No service level applies unless expressly identified as such in the applicable Service Definition or Order .
SOC – Security Operations Centre	A team or facility responsible for monitoring, investigating and responding to cybersecurity events and threats.
Supported Asset	A device, system, service or other technology asset that meets the Supplier's applicable support requirements and is expressly within the scope of a Service.
Ticket	A record created within the Supplier's service-management system relating to an Incident, Service Request, Change or other support activity.
Users	A defined list of employees or authorised contacts who are entitled to support under the contracted services .



Unsupported / End-of-Life (EOL)

Hardware, **software** or a service that is no longer supported by its manufacturer/vendor, is outside the **Supplier's** supported standards, or cannot reasonably receive required security or maintenance updates.

Virtual Machine (VM)

A **software**-defined computer operating within a virtualisation platform and running its own operating system. A VM may constitute a separate Server where it is independently managed under a Service.

VPN – Virtual Private Network

Technology providing an encrypted connection between an authorised device, user, site or network and another network or service.

Zero-Day Vulnerability

A **software** or hardware vulnerability for which an effective vendor fix or Patch may not yet be generally available at the time the vulnerability becomes known or exploited.