

The top half of the page features an abstract background composed of various shades of green and teal. These colors are arranged in a complex, low-poly geometric pattern that resembles a stylized, crystalline structure or a series of overlapping planes. The pattern is more dense and darker in the upper left and right corners, fading into a lighter, more transparent green towards the bottom left.

Master Services Agreement



Contents

1. Parties Involved	3
2. Agreement	3
3. Agreed Terms	3
4. Scope of Services	4
5. Service Levels and Performance Metrics.....	15
6. Third-Party Services.....	15
7. Payment Terms	16
8. Term and Termination.....	16
9. Confidentiality	18
10. Intellectual Property Rights	19
11. Non-Disclosure and Confidentiality	19
12. Limitation of Liability.....	19
13. Dispute Resolution	20
14. Force Majeure	21
15. Governing Law	22
16. Jurisdiction.....	22
17. Entire Agreement.....	22
18. Amendments	22
19. Survivability.....	22
20. Signatures	22

1. Parties Involved

THIS AGREEMENT is dated

PARTIES

MSP: OGEL IT LTD which has its registered office at Unit 4 Meadway Court, Rutherford Close, Stevenage, Herts, SG1 2EF

Client: <NAME>,<ADDRESS> (referred to as "you" and "your")

- A. We are an independent managed service provider (**MSP**) in the business of providing the delivery of outsourced IT management functions to business.
- B. We agree to provide our **MSP** services to you on the terms set out herein.

(each a "**Party**" and together the "**Parties**").

2. Agreement

In consideration of the mutual benefits, it is hereby agreed that you will appoint us as your managed service provider to provide the services outlined in our **proposal** subject to the following **Terms and Conditions**.

3. Agreed Terms

3.1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement

Commencement Date	The date of this agreement as detailed in Clause 1.
Confidential Information	For the purposes of this Agreement, "Confidential Information" means any and all information disclosed by either party to the other, whether orally, in writing, electronically, or in any other form, 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, without limitation, business plans, financial data, pricing, customer lists, technical information, trade secrets, know-how, software, documentation, security procedures, and any other proprietary information relating to the disclosing party's operations. Confidential Information does not include information that: (a) is or becomes publicly available through no fault of the receiving party; (b) was lawfully known to the receiving party prior to disclosure; (c) is lawfully obtained by the receiving party from a third party without restriction; or (d) is independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information.
Contract Variation Notice	A document detailing a variation to this agreement signed by both parties.
Good Industry Practice	Means the exercise of that degree of care, skill, diligence, prudence, efficacy, foresight and timeliness which would reasonably be expected at

	such time from a leading and expert provider of services similar to the Services to a customer like the Client , such provider seeking to comply with its contractual obligations in full and complying with all applicable Laws.
Law	Means any law, statute, subordinate legislation within the meaning of section 21(1) Interpretation Act 1978, by-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives of requirements of any regulatory body with which the Authority or Contractor is bound to comply.
Liabilities	Means any actions, costs, claims, charges, liabilities, demands, fines, penalties, damages, compensation, losses, awards or expenses (including legal and other reasonable professional costs and expenses).
MSP personnel	Means any directors, officers, employees, staff, agents, consultants and contractors engaged by the Contractor in connection with this Agreement.
MSP-licensed software	Software purchased and licenses by the MSP for its own use in the delivery of services to the Client.
Proposal	A separate document produced by the MSP and issued to the Client detailing the service proposed and associated costs.
Services	As defined in 4 Scope of Services delivered by the MSP to the Client.
Subcontractor	Means any entity engaged by the MSP to perform the Services.
Subcontractor Personnel	Means any directors, officers, employees, staff, agents, consultants and contractors engaged by any Subcontractor in connection with this Agreement.
Termination Notice	Means a written notice of termination given by the Client to the MSP, notifying the MSP of the intention of Client to terminate this Agreement with immediate effect or on a later date the Client specifies and setting out the grounds for termination.
Third-party supplier	Refers to any vendor, manufacturer, supplier or sub-contractor used by the MSP internally or as part of the delivery of services.
Transfer Period	Refers to an agreed period between Client and MSP for the transition to another a supplier, in the absence of any agreement this is a minimum of 30 days.
UK Data Protection Legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including, but not limited to, the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SU 2003/2426) as amended.
Working Day	Means any day other than a Saturday, Sunday or a public holiday in England, Wales and Scotland.

4. Scope of Services

The following table provides a summary of the services included within the scope of this agreement.

Service	Scope
End User Compute (EUC) Management	

End User Services (Helpdesk & ITSM)	
Managed Microsoft 365 Tenant	
Managed Microsoft 365 Backup	
Account Management	
License Management	
Server Support	
Network Management	
Onsite Engineering	
Licensing Procurement	
Hardware Procurement	

4.1. End User Compute (EUC) Management

To provide management and support for the **Client's** end-user computing environment, including desktops, laptops, mobile devices, and associated applications, ensuring secure, reliable, and optimised user experience.

4.1.1. Device Provisioning & Configuration

- (a) Deploy and configure desktops, laptops, and mobile devices according to **Client** standards.
- (b) Apply operating system hardening and security best practices.
- (c) Install and configure approved applications and productivity tools.

4.1.2. Patch Management & Updates

- (a) Regularly publish operating system patches to maintain security and compliance.
- (b) Regularly publish application patches for the following applications:

Office Productivity	Microsoft Office (Word, Excel, PowerPoint, Outlook, Teams, OneDrive), Microsoft Visio, Microsoft Project, Creative Cloud, Acrobat Reader, Acrobat Pro, Photoshop, InDesign, Illustrator
Web Browsing	Google Chrome, Microsoft EDGE
Conferencing	Zoom, Teams
VPN	FortiClient
Antivirus/Antimalware	Microsoft Defender
Backup	NinjaRMM
File Sync	OneDrive

- (c) Validate updates in a controlled environment before deployment where possible.
- (d) Maintain patching schedules and compliance reports where these have been agreed with the **Client**.

4.1.3. Endpoint Security

- (a) Implement antivirus, endpoint protection, and encryption solutions.
- (b) Enforce policies for device access, password management, and MFA.
- (c) Monitor for vulnerabilities and remediate where appropriate.

- 4.1.4. Monitoring & Performance Management
 - (a) Monitor device health, performance, and resource utilisation.
 - (b) Generate alerts for hardware failures or performance degradation.
 - (c) Take corrective actions to maintain optimal user experience.
- 4.1.5. Incident & Service Request Management
 - (a) Provide helpdesk support for end-user issues.
 - (b) Manage incidents and service requests per agreed SLAs.
 - (c) Perform root cause analysis for recurring problems.
- 4.1.6. Asset & Lifecycle Management
 - (a) Maintain an accurate inventory of all end-user devices.
 - (b) Manage device lifecycle from procurement to decommissioning.
 - (c) Ensure secure disposal of retired devices.
- 4.1.7. Backup & Data Protection
 - (a) Implement backup solutions for user data where applicable.
 - (b) Support data recovery in case of device failure or loss.
 - (c) Validate backup integrity and compliance with **Client** policies.
- 4.1.8. Reporting & Documentation
 - (a) Deliver quarterly EUC health and performance reports.
 - (b) Maintain configuration and change logs.

4.2. End User Services (Remote Helpdesk & ITSM)

To deliver a UK-based remote helpdesk service and IT Service Management (ITSM) toolset that provides comprehensive support for end users, ensuring timely resolution of incidents, effective change management, and improved user experience.

- 4.2.1. Service Hours & Availability
 - Operating Hours: Monday to Friday, 08:00 – 18:00 (UK time).
 - Exclusions: UK weekends and UK public/bank holidays.
 - Contact Channels:
 - Telephone
 - Email
 - Self-Service Portal
- 4.2.2. Helpdesk Services
 - (a) Incident Management
 - (b) Logging, categorisation, and prioritisation of incidents.
 - (c) Remote troubleshooting and resolution of end-user issues.
 - (d) Escalation to second/third-line support or vendors as required.
- 4.2.3. Problem Management
 - (a) Identification and analysis of recurring issues.
 - (b) Root cause analysis and implementation of permanent fixes.
 - (c) Maintenance of known error database.
- 4.2.4. Change Management

- (a) Processing and approval of standard and emergency changes.
 - (b) Coordination of change implementation with minimal business disruption.
 - (c) Documentation of all changes for audit and compliance.
- 4.2.5. Knowledge Management
 - (a) Development and maintenance of a knowledge base for common issues.
 - (b) Accessible via self-service portal for end users.
 - (c) Continuous improvement based on incident trends.
- 4.2.6. ITSM Toolset Delivery
 - (a) Self-Service Portal:
 - (b) End users can log incidents, request services, and track progress.
- 4.2.7. Incident & Problem Management
 - (a) Full lifecycle management of incidents and problems.
- 4.2.8. Change Management
 - (a) Workflow-driven change approval and implementation.
- 4.2.9. Knowledge Base
 - (a) Searchable repository of solutions and FAQs.
- 4.2.10. Reporting & Communication
 - (a) Quarterly service performance reports including;
 - (i). Incident volumes and resolution times,
 - (ii). SLA compliance,
 - (iii). Problem and change management metrics.
 - (b) Quarterly service reviews with the **Client** where agreed.

4.3. Managed Microsoft 365 Tenant

To provide ongoing administration, monitoring, and support for the **Client's** Microsoft 365 environment, ensuring optimal performance, security, and compliance while enabling efficient collaboration and productivity.

- 4.3.1. Tenant Administration
 - (a) Manage Microsoft 365 tenant settings and configurations.
 - (b) Maintain domains, subscriptions, and license allocations.
 - (c) Apply Microsoft best practices for governance and security.
- 4.3.2. User & Group Management
 - (a) Create, modify, and remove user accounts and groups.
 - (b) Assign and manage licenses based on **Client** requirements.
 - (c) Implement role-based access controls.
- 4.3.3. Security & Compliance
 - (a) Enforce Multi-Factor Authentication (MFA) and Conditional Access policies.
 - (b) Monitor and maintain compliance centre configurations (DLP, retention policies).

- (c) Regularly review and update security settings to mitigate risks.
- 4.3.4. Email & Collaboration Services
 - (a) Manage Exchange Online mail flow, connectors, and transport rules.
 - (b) Configure and maintain Teams policies and settings.
 - (c) Oversee SharePoint and OneDrive sharing permissions and storage quotas.
- 4.3.5. Monitoring & Reporting
 - (a) Monitor service health and performance via Microsoft 365 Admin Center.
 - (b) Provide quarterly reports on tenant health, license usage, and security posture.
 - (c) Alert **Client** of critical issues and provide remediation steps.
- 4.3.6. Support & Incident Management
 - (a) Provide helpdesk support for Microsoft 365-related issues.
 - (b) Manage escalations with Microsoft support when required.
 - (c) Ensure timely resolution of incidents per agreed SLAs.
- 4.3.7. Change Management
 - (a) Implement approved configuration changes and updates.
 - (b) Communicate upcoming Microsoft feature changes and their impact.
 - (c) Assist with adoption of new Microsoft 365 capabilities.

4.4. Managed Microsoft 365 Backup

To provide a secure, reliable, and compliant backup solution for the **Client's** Microsoft 365 tenant, ensuring protection of critical data across Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.

- 4.4.1. Backup Solution Deployment
 - (a) Implement and configure a Microsoft 365 backup platform approved by the **Client**.
 - (b) Integrate with Exchange Online, SharePoint Online, OneDrive, and Teams.
 - (c) Validate connectivity and initial backup completion.
- 4.4.2. Backup Policy Configuration
 - (a) Define retention policies based on **Client** requirements and compliance standards.
 - (b) Configure backup schedules (daily, weekly, or custom intervals).
 - (c) Apply encryption and secure storage protocols.
- 4.4.3. Data Coverage
 - Backup of:
 - (a) Exchange Online: Mailboxes, calendars, contacts.
 - (b) SharePoint Online: Sites, document libraries, lists.
 - (c) OneDrive for Business: User files and folders.
 - (d) Microsoft Teams: Chats, files, and associated SharePoint data.
- 4.4.4. Monitoring & Maintenance

- (a) Monitor backup jobs for success and failures.
 - (b) Perform annual integrity checks and validation of backup data.
- 4.4.5. Restore Services
 - (a) Provide granular restore capabilities (individual items, folders, or entire workloads).
 - (b) Support point-in-time recovery for compliance and disaster recovery scenarios.
 - (c) Ensure restoration meets agreed SLAs.
- 4.4.6. Reporting
 - (a) Deliver quarterly backup status reports.
 - (b) Highlight any issues or anomalies with remediation actions.

4.5. Account Management

To provide strategic and operational account management services that ensure alignment between the **Client's** business objectives and the Managed IT Services delivered by the **MSP**, fostering a collaborative relationship and continuous improvement.

- 4.5.1. Primary Account Manager
 - (a) Assign a primary Account Manager as the **Client's** main point of contact.
 - (b) Serve as liaison between **Client** stakeholders and **MSP** technical teams.
- 4.5.2. Strategic Planning & Alignment
 - (a) Conduct regular business reviews (quarterly or as agreed).
 - (b) Align IT services with **Client's** business goals and technology roadmap.
 - (c) Identify opportunities for optimisation and innovation.
- 4.5.3. Service Performance Management
 - (a) Review SLA compliance and service delivery metrics.
 - (b) Address recurring issues and implement corrective actions.
 - (c) Provide escalation management for critical incidents.
- 4.5.4. Financial & Contract Management
 - (a) Monitor service consumption and billing accuracy.
 - (b) Manage renewals, amendments, and contract compliance.
 - (c) Provide budget forecasting for IT services.
- 4.5.5. Communication & Reporting
 - (a) Deliver quarterly account reports summarising:
 - (i). Metrics from other in scope services;
 - (ii). Business review outputs;
 - (iii). Service consumption/billing information.
 - (b) Communicate upcoming changes, risks, and recommendations.

4.6. License Management

To provide management of software and cloud service licenses, assisting with compliance, cost optimisation, and alignment with the **Client's** operational needs.

- 4.6.1. License Inventory & Tracking
 - (a) Maintain an up-to-date inventory of all software and cloud service licenses under **MSP** management.
 - (b) Track license usage and allocation across **Client** systems and users.
- 4.6.2. Procurement & Renewal Management
 - (a) Coordinate acquisition of new licenses based on **Client** requirements.
 - (b) Manage license renewals to prevent service interruptions.
 - (c) Negotiate with vendors for optimal pricing and terms.
- 4.6.3. Compliance & Audit Support
 - (a) Ensure adherence to vendor licensing agreements and legal requirements within scope of the services delivered by the **MSP**.
 - (b) Provide documentation and reports for internal or external audits.
 - (c) Identify and remediate any compliance risks.
- 4.6.4. Optimisation & Cost Control
 - (a) Analyse license utilisation to identify underused or redundant licenses.
 - (b) Recommend consolidation or alternative licensing models to reduce costs.
 - (c) Provide forecasting for future license needs based on growth and usage trends.
- 4.6.5. Reporting & Communication
 - (a) Deliver monthly or quarterly license management reports, including:
 - (i). Current license inventory;
 - (ii). Usage statistics;
 - (iii). Notification of upcoming renewals.

4.7. Server Support

To provide proactive management, monitoring, and support for the **Client's** physical and virtual server infrastructure, ensuring high availability, security, and optimal performance.

- 4.7.1. Server Provisioning & Configuration
 - (a) Deploy and configure physical and virtual servers according to **Client** requirements.
 - (b) Apply standard operating system hardening and security best practices.
 - (c) Configure storage, networking, and virtualisation settings.
- 4.7.2. Monitoring & Performance Management
 - (a) Implement 24/7 monitoring for server health, resource utilisation, and availability.
 - (b) Track CPU, memory, disk, and network performance metrics.
 - (c) Generate alerts and take corrective actions for anomalies.
- 4.7.3. Patch Management & Updates

- (a) Apply operating system and firmware updates on a scheduled basis.
 - (b) Validate patches in a test environment before production deployment.
 - (c) Maintain compliance with security and regulatory standards.
- 4.7.4. Backup & Disaster Recovery
 - (a) Configure and manage server backups according to **Client** policies.
 - (b) Perform regular backup integrity checks.
 - (c) Support disaster recovery planning and execution.
- 4.7.5. Security Management
 - (a) Implement antivirus, endpoint protection, and intrusion detection measures.
 - (b) Enforce access controls and role-based permissions.
 - (c) Monitor for vulnerabilities and apply remediation promptly.
- 4.7.6. Incident & Problem Management
 - (a) Respond to server-related incidents per agreed SLAs.
 - (b) Perform root cause analysis for recurring issues.
 - (c) Document and implement permanent fixes.
- 4.7.7. Capacity Planning & Optimisation
 - (a) Review resource utilisation trends.
 - (b) Recommend hardware upgrades or virtualisation adjustments.
 - (c) Provide forecasting for future infrastructure needs.
- 4.7.8. Reporting & Documentation
 - (a) Deliver quarterly reports including:
 - (i). Infrastructure health reports;
 - (ii). Maintain configuration and change logs;
 - (iii). Patch & Update Logs;
 - (iv). Backup & Recovery Status Reports;
 - (v). Incident & Resolution Documentation.

4.8. Network Management

To provide comprehensive management, monitoring, and support for the **Client's** network infrastructure, ensuring secure, reliable, and optimised connectivity across all locations.

- 4.8.1. Network Monitoring & Performance Management
 - (a) Implement 24/7 monitoring of routers, switches, firewalls, and wireless access points.
 - (b) Track bandwidth utilisation, latency, and packet loss where agreed.
 - (c) Generate alerts and take corrective actions for performance issues.
- 4.8.2. Configuration & Change Management
 - (a) Maintain and update network device configurations.
 - (b) Apply firmware and security patches to network equipment.
 - (c) Document all changes for compliance and audit purposes.

- 4.8.3. Security Management
 - (a) Configure and manage firewalls, VPNs, and intrusion prevention systems.
 - (b) Enforce network access controls and segmentation.
 - (c) Monitor for vulnerabilities and apply remediation promptly.
- 4.8.4. Incident & Problem Management
 - (a) Respond to network-related incidents per agreed SLAs.
 - (b) Perform root cause analysis for recurring connectivity issues.
 - (c) Implement permanent fixes and preventive measures.
- 4.8.5. Capacity Planning & Optimisation
 - (a) Review network utilisation trends.
 - (b) Recommend upgrades or adjustments to support growth and performance.
 - (c) Provide forecasting for future bandwidth and hardware needs.
- 4.8.6. Backup & Disaster Recovery
 - (a) Backup network device configurations regularly.
 - (b) Support network recovery in case of failure or disaster.
 - (c) Validate recovery procedures through periodic testing.
- 4.8.7. Reporting & Documentation
 - (a) Deliver quarterly reports including:
 - (i). Health and performance reports;
 - (ii). Maintain network topology diagrams and configuration logs;
 - (iii). Network Health & Performance Reports;
 - (iv). Configuration Backup & Change Logs;
 - (v). Incident & Resolution Documentation;
 - (vi). Capacity Planning Recommendations.

4.9. Onsite Engineering

To provide skilled onsite engineering support for the **Client's** IT infrastructure and end-user environment, ensuring timely resolution of issues that cannot be addressed remotely such as supporting planned maintenance or project activities.

- 4.9.1. Incident Resolution
 - (a) Attend onsite to resolve hardware failures, network issues, or complex problems escalated from the remote helpdesk.
 - (b) Perform diagnostics and repairs on servers, network devices, and end-user equipment.
 - (c) Coordinate with vendors for warranty repairs or replacements.
- 4.9.2. Preventive Maintenance
 - (a) Conduct scheduled health checks of onsite equipment.
 - (b) Document maintenance activities.
- 4.9.3. Installations & Upgrades

- (a) Deploy new hardware (servers, switches, desktops, laptops).
 - (b) Perform system migrations and upgrades as per **Client** requirements.
- 4.9.4. Project Support
 - (a) Provide onsite assistance for IT projects such as office moves, infrastructure refresh, or technology rollouts.
 - (b) Work under **MSP** project management guidelines to ensure timely delivery.
- 4.9.5. Security & Compliance
 - (a) Implement physical and logical security measures during onsite activities.
 - (b) Ensure adherence to **Client's** security and compliance policies.
- 4.9.6. Documentation & Reporting
 - (a) Record all onsite activities in the ITSM system.
 - (b) Provide detailed reports for incidents, changes, and project tasks.
 - (c) Maintain asset records for any hardware changes.
- 4.9.7. Service Parameters
 - (a) **Scheduling:** Onsite visits arranged via the **MSP** helpdesk or account manager.
 - (b) **Coverage:** As specified within the associated **proposal**.
 - (c) **Availability:** Standard business hours except where additional hours are specified in the **proposal**.
 - (d) **Response Times:** Aligned with standard SLAs excluding travel time to site where required unless otherwise specified within the **proposal**.

4.10. Licensing Procurement

To provide end-to-end management of software and cloud service license procurement for the **Client**, ensuring timely acquisition, cost Optimisation, and compliance with vendor requirements.

- 4.10.1. Requirements Gathering
 - (a) Work with the **Client** to identify licensing needs based on current and future requirements.
 - (b) Validate compatibility with existing infrastructure and applications.
- 4.10.2. Vendor Engagement & Quotation
 - (a) Source licenses from approved vendors or distributors.
 - (b) Obtain competitive quotations and negotiate favourable terms.
 - (c) Ensure vendor compliance and authenticity of licenses.
- 4.10.3. License Acquisition
 - (a) Purchase licenses on behalf of the **Client** under agreed commercial terms.
 - (b) Manage delivery of license keys, activation codes, or subscription credentials.
 - (c) Validate successful activation and deployment.
- 4.10.4. Renewal Management
 - (a) Track license expiry dates and renewal schedules.
 - (b) Notify **Client** of upcoming renewals and provide cost estimates.

- (c) Process renewals to avoid service disruption.
- 4.10.5. Compliance & Documentation
 - (a) Maintain records of all purchased licenses and agreements.
 - (b) Provide documentation for audits and compliance checks.
 - (c) Ensure adherence to vendor licensing terms and conditions.
- 4.10.6. Cost Optimisation
 - (a) Review license usage and recommend consolidation or alternative models.
 - (b) Identify opportunities for volume discounts or subscription adjustments.
- 4.10.7. Reporting
 - (a) Deliver quarterly procurement and license status reports.
 - (b) Highlight upcoming renewals and budget forecasts.

4.11. Hardware Procurement

To provide end-to-end management of IT hardware procurement for the **Client**, ensuring timely delivery, cost efficiency, and compatibility with the **Client's** technical and business requirements.

- 4.11.1. Requirements Analysis
 - (a) Collaborate with the **Client** to identify hardware needs (servers, networking equipment, desktops, laptops, peripherals).
 - (b) Validate specifications against existing infrastructure and future scalability requirements.
- 4.11.2. Vendor Engagement & Quotation
 - (a) Source hardware from approved vendors or distributors.
 - (b) Obtain competitive quotations and negotiate favourable pricing and terms.
 - (c) Ensure vendor compliance and authenticity of products.
- 4.11.3. Procurement & Order Management
 - (a) Place orders on behalf of the **Client** under agreed commercial terms.
 - (b) Track order status and manage delivery timelines.
 - (c) Validate hardware upon receipt for accuracy and quality.
- 4.11.4. Warranty & Support Management
 - (a) Register hardware warranties with vendors.
 - (b) Maintain records of warranty periods and support entitlements.
 - (c) Assist with warranty claims and replacements when required.
- 4.11.5. Asset Tagging & Documentation
 - (a) Tag and record all procured hardware in the **Client's** asset inventory.
 - (b) Provide detailed documentation for audit and compliance purposes.
- 4.11.6. Cost Optimisation
 - (a) Recommend cost-effective alternatives without compromising quality.
 - (b) Identify opportunities for bulk purchasing or vendor discounts.
- 4.11.7. Reporting

- (a) Deliver monthly or quarterly procurement reports.
- (b) Highlight upcoming hardware refresh cycles and budget forecasts.

5. Service Levels and Performance Metrics

5.1. The Supplier shall:

- 5.1.1. prioritise all Support Requests based on its reasonable assessment of the severity level of the problem reported; and
- 5.1.2. resolve all Support Requests in accordance with the responses and resolution times specified in the table set out below:

Priority	Response	Resolution	Definition
P1	30 mins	4 hours	Critical Severity issue affecting all users or multiple services, resulting in offline / affected services.
P2	1 hour	8 hours	High-severity issue affecting a large group of users / a single business unit, or a single service being offline.
P3	4 hours	3 days	Medium Severity issue affecting a small group of users or an individual, impacting the service's resilience.
P4	1 day	5 days	Single-user low-priority issues and service requests.

6. Third-Party Services

Third party services are products or services that are not exclusively operated or controller by the **MSP** or that involve significant participation from an entity outside of the **MSPs** control. The **MSP** utilises a number of third-party services to assist in providing **services** to the **Client**.

The following table lists the third-party services that may be used by the **MSP**, along with links to each third-party services providers agreements and policies.

Provider	Service	Website
NinjaRMM	Remote Monitoring and Management	https://www.ninjaone.com/terms-of-use/ https://www.ninjaone.com/license-agreement/ https://www.ninjaone.com/privacy-policy/
HALO ITSM	- Incident Management - Knowledge Base - Self-service portal - Change Control - Service Catalogue - CMDB/Configuration Management	https://usehalo.com/terms-and-conditions https://usehalo.com/privacy-policy
Microsoft 365	- Online collaboration Services - IaaS/SaaS/PaaS provider - Antivirus	https://www.microsoft.com/licensing/docs/custom eragreement.
CIPP	M365 tenant	https://go.cyberdrain.com/msa

	management	
--	------------	--

7. Payment Terms

All payments shall be made within thirty (30) days from the date the invoice is issued. In the event that payment is not received within this period, a late payment fee of 1.5% per month will be applied to the outstanding balance until full payment is made. The applicable fees are as detailed in the proposal and as part of any additional service requests or contract variations agreed between the parties.

8. Term and Termination

8.1. Term

8.1.1. This Agreement shall commence on the **Commencement Date** and shall continue for a minimum of 12 months (the "Initial Term"), unless otherwise terminated in accordance with **8.2 Termination**, and subject always to the terms of any relevant Transfer Period.

8.1.2. Upon expiry of the Initial Term, the Agreement shall automatically continue on a rolling ninety (90) day basis unless and until terminated by the **Client** in accordance with Clause **8.2 Termination** and any **Transfer Period**.

8.1.3. The purchase of any licensing or subscription services from or via the **MSP** by the **Client** will be subject to the terms and conditions referenced as part of that purchase agreement. For Microsoft licensing and subscription services please refer to the Microsoft Customer Agreement:

<https://www.microsoft.com/licensing/docs/customeragreement>

8.2. Termination

8.2.1. Either party may terminate this Agreement:

- (a) for convenience, upon providing ninety (90) days' prior written notice to the other party following the expiration of the **Initial Term**;
- (b) immediately, if the other party commits a material breach of this Agreement and fails to remedy such breach within fifteen (15) days of receiving written notice;
- (c) immediately, if the other party becomes insolvent, enters into bankruptcy, or ceases to carry on business;
- (d) if a Force Majeure Event occurs for a continuous period of more than 90 days.

8.2.2. Upon termination, the Client shall remain liable for all fees and charges accrued up to the effective date of termination, including any outstanding invoices and costs associated with services rendered. Obligations relating to confidentiality, intellectual property, and payment of fees shall survive termination of this Agreement.

8.2.3. On termination or expiry of this Agreement for any reason (unless otherwise provided within the **proposal** or **contract variation notice**).

- (a) The **MSP** shall return all the **Client's** Confidential Information to the **Client**,

and destroy or permanently erase (to the extent technically practicable) all copies of the **Client's** Confidential Information made by the **MSP** and the **MSP** shall use reasonable endeavours to ensure that anyone to whom the **MSP** has supplied Confidential Information destroys or permanently erases (to the extent technically practicable) such Confidential Information and any copies made by them, within such reasonable timeframe as specified by the **Client** and comply with **12 Non-Disclosure and Confidentiality**;

- (b) any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this Agreement, which existed at or before the date of termination, shall not be affected or prejudiced; and
- (c) clauses 9, 10, 12, 13, 14 and any other provision of this Agreement that either expressly or by implication has effect after termination shall remain in force.

9. Warranties

9.1. MSP

The MSP represents and warrants that:

- 9.1.1. it is validly incorporated, organised and subsisting in accordance with the Laws of its place of incorporation;
- 9.1.2. it has full capacity and authority to enter into and perform its obligations under this Agreement;
- 9.1.3. this Agreement is executed by its duly authorised representative(s);
- 9.1.4. all written statements and representations in any written submissions made by the **MSP** as part of the procurement process, in the proposal and any other documents submitted remain true and accurate except to the extent that such statements and representations have been expressly superseded or varied by this Agreement or to the extent that the **MSP** has otherwise disclosed to the **Client** in writing prior to the **Commencement Date**;
- 9.1.5. it will perform the **Services** with all due professional skill, care and diligence, in a timely and efficient manner, using appropriately qualified and experienced Contractor Personnel and in accordance with **Good Industry Practice** and applicable Law;
- 9.1.6. it has obtained and will maintain appropriate levels of insurance of all risks and liabilities which may be incurred by the **MSP** pursuant to this Agreement and it shall provide reasonable evidence of this to the **Client** within five (5) Working Days of a request by the **Client**.

9.2. CLIENT

The Client represents and warrants that:

- 9.2.1. it has full capacity and authority to enter into and perform its obligations under this Agreement;
- 9.2.2. this Agreement is executed by its duly authorised representative(s);
- 9.2.3. it shall comply with all applicable Laws and regulations with respect to its

obligations under this Agreement; and

- 9.2.4. it has obtained and will maintain all necessary consents, approvals, licences or authorisations required for the performance of its obligations under this Agreement.
- 9.3. The representations and warranties set out in Clause 9.1 shall be deemed to be repeated by the **MSP** on the Commencement Date by reference to the facts then existing.
- 9.4. Each of the representations and warranties set out in Clauses **9.1** and **9.2** shall be construed as a separate representation and warranty and shall not be limited or restricted by reference to, or inference from, the terms of any other representation, warranty or any other undertaking in this Agreement.
- 9.5. If at any time a Party becomes aware that a representation or warranty given by it under Clauses **9.1** and **9.2** respectively has been breached, is untrue or is misleading, it shall immediately notify the other Party of the relevant occurrence in sufficient detail to enable the other Party to make an accurate assessment of the situation.
- 9.6. The fact that any provision of this Agreement is expressed as a warranty shall not preclude any right of termination which the **Client** may have in respect of breach of that provision by the **MSP**.

10. Confidentiality

- 10.1. The **MSP** agrees to hold the Confidential Information in confidence and safeguard it accordingly with security measures and the degree of care required by Good Industry Practice, and shall not:
 - 10.1.1. disclose any Confidential Information to any third party, save to the extent permitted under this 10 Confidentiality; or
 - 10.1.2. use or otherwise exploit the Confidential Information for any purpose other than the purposes anticipated under this Agreement.
- 10.2. To the extent that it is necessary for the **MSP** to disclose Confidential Information to its **MSP personnel** and **Subcontractors** (including **Subcontractor personnel** to enable the performance of its obligations under this Agreement, the Contractor shall ensure that such **MSP personnel** and **Subcontractors** (including **Subcontractor personnel**) are subject to obligations no less onerous than those set out in this **10 Confidentiality** in respect of all Confidential Information.
- 10.3. Clause 10.1 shall not apply to information which:
 - 10.3.1. is or becomes public knowledge (otherwise than as a direct or indirect result of any breach of this Agreement or a breach of an obligation of confidentiality);
 - 10.3.2. is lawfully obtained and is in the possession of the **MSP**, without restriction as to its disclosure, before receiving it from the **Client**, which as far as the **MSP** is aware has not been obtained in breach of, and is not otherwise subject to, any obligation of confidentiality;
 - 10.3.3. is required by Law to be disclosed; or
 - 10.3.4. was independently developed by the **MSP** without access to the Confidential Information, where such independent development can be shown by written evidence.

- 10.4. The **MSP** may disclose the Confidential Information:
- 10.4.1. to the extent that it has the prior written consent of the **Client**;
 - 10.4.2. to the extent that such Confidential Information is required to be disclosed by Law, by any governmental or other regulatory authority or by a court or other authority of competent jurisdiction, provided that, to the extent it is legally permitted to do so, it gives the **Client** as much notice of disclosure as possible, and where notice of disclosure is not prohibited and is given in accordance with this Clause **10 Confidentiality**, it takes into account the reasonable requests of the **Client** in relation to the content of such disclosure; or
 - 10.4.3. on a confidential basis, no less stringent than the obligations of confidentiality to which it is bound under this Agreement, to its auditors or professional advisers.
- 10.5. The obligations contained in this Clause **10 Confidentiality** shall continue to apply after the expiry or termination of this Agreement.

11. Intellectual Property Rights

- 11.1. Upon termination or expiration of this Agreement, the **Client** shall immediately cease using any **MSP-licensed** software and shall allow the **MSP** to remove or disable such software from all **Client** devices and systems. The **Client** agrees to cooperate fully with the **MSP** to ensure complete removal within 30 days of termination.
- 11.2. All writings, works of authorship, or other materials created by either the **MSP** or the **Client** in connection with the Services (collectively, "Provider Work") shall be owned exclusively by the **MSP**. For any **MSP-owned** intellectual property that resides on the **Client's** devices, the **MSP** grants the **Client** a limited, non-exclusive, non-transferable license to use such intellectual property solely for the duration of the applicable Order or Service Attachment. This license shall automatically terminate upon expiration or termination of the related Order or Service Attachment, at which time the **Client** must cease all use and allow removal of such intellectual property.
- 11.3. The **MSP** reserves the right, at its sole discretion, to replace, upgrade, or substitute any equipment, hardware, or software used in the provision of Services, provided that such changes do not materially degrade the agreed service levels or functionality. The **MSP** shall notify the **Client** of any significant changes that may impact the **Client's** environment or require cooperation for implementation.

12. Non-Disclosure and Confidentiality

- 12.1. Both the **MSP** and the **Client** acknowledge that, in the course of performing the **Services**, they may encounter confidential or proprietary information belonging to the other party. Each party agrees to maintain such information in strict confidence and not disclose it to any third party, except as required by law or with prior written consent of the disclosing party.

13. Limitation of Liability

- 13.1. The following provisions set out the entire limitations on the financial liability of the Parties (including any Liability for the acts or omissions of its **MSP personnel**, any

Subcontractors and any **Subcontractor personnel**) to the other in respect of:

- 13.1.1. any breach of this Agreement howsoever arising; and
- 13.1.2. any representation, misrepresentation (whether innocent or negligent), statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.
- 13.2. Nothing in this Agreement excludes either Party's liability (including any liability for the acts or omissions of its Contractor Personnel, any Subcontractors and any Subcontractor Personnel):
 - 13.2.1. for death or personal injury caused by that Party's negligence;
 - 13.2.2. for fraud or fraudulent misrepresentation or theft or criminal activity; or
 - 13.2.3. any other matter which, by Law, may not be excluded or limited.
- 13.3. Subject to Clauses **13.2**:
 - 13.3.1. Neither **Party** nor the **MSPs Third-Party Suppliers** shall in any circumstances be liable, whether in tort (including for negligence or breach of statutory duty howsoever arising), contract, misrepresentation (whether innocent or negligent) or otherwise for:
 - (a) loss of profits;
 - (b) loss of business;
 - (c) loss of revenue;
 - (d) loss of or damage to goodwill;
 - (e) loss of savings (whether anticipated or otherwise);
 - (f) pure economic loss; and/or
 - (g) any indirect, special or consequential loss or damage.
 - 13.3.2. The limitation of each **Party's** total liability in contract, tort (including negligence or breach of statutory duty howsoever arising), misrepresentation, (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited per claim to 125% of charges in the preceding twelve months of the Term, of any other sum as may be agreed in writing between both **Parties**.
 - 13.3.3. Nothing in this Agreement shall impose any liability on any member of the staff of either **Party** or its representatives in their personal capacity.

14. Dispute Resolution

- 14.1. The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with this Agreement.
- 14.2. If the Parties cannot resolve the dispute pursuant to Clause **14.1** the dispute may, by agreement between the Parties, be referred to mediation pursuant to Clause **14.4**.
- 14.3. The performance of the Services shall not cease or be delayed by the reference of a dispute to mediation pursuant to Clause **14.4**.
- 14.4. If the Parties agree to refer the dispute to mediation:
 - 14.4.1. in order to determine the person who shall mediate the dispute (the "Mediator") the Parties shall by agreement choose a neutral adviser or mediator from one of the dispute resolution providers listed by the Government Procurement Service

on its website or in its printed guidance on dispute resolution within 20 Working Days after agreeing to refer the dispute to mediation;

- 14.4.2. the Parties shall within 10 Working Days of the appointment of the Mediator meet with the Mediator to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations to be held. If considered appropriate, the Parties may at any stage seek assistance from the Government Procurement Service to provide guidance on a suitable procedure;
 - 14.4.3. unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings;
 - 14.4.4. if the Parties reach agreement on the resolution of the dispute within 30 Working Days of the Mediator being appointed, or such longer period as may be agreed in writing between the Parties, the agreement shall be reduced to writing and shall be binding on the Parties once it is signed by both the **Client** and the Contractor; and
 - 14.4.5. failing agreement within 30 Working Days of the Mediator being appointed, or such longer period as may be agreed in writing between the Parties, either of the Parties may invite the Mediator to provide a non-binding but informative opinion in writing. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to this Agreement without the prior written consent of both Parties.
- 14.5. If the Parties do not agree to refer the dispute to mediation, or if the **Parties** fail to reach agreement as to who shall mediate the dispute pursuant to Clause **14.4.1**, or if they fail to reach agreement in the structured negotiations within 30 Working Days of the Mediator being appointed or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the courts of England and Wales.

15. Force Majeure

- 15.1. Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from a Force Majeure Event. In such circumstances, the affected Party shall be entitled to a reasonable extension of the time for performing such obligations, provided that:
- 15.1.1. as soon as reasonably practicable after the start of the Force Majeure Event, it notifies the other Party in writing of the Force Majeure Event, the date on which it started, its likely or potential duration, and the effect of the Force Majeure Event on its ability to perform any of its obligations under this Agreement;
 - 15.1.2. uses all reasonable endeavours to overcome and mitigate the effect of the Force Majeure Event on the performance of its obligations as soon as reasonably practicable, including actively managing any problems caused or contributed to by any third party;
 - 15.1.3. it carries out its duties to the best level reasonably achievable in the circumstances of the Force Majeure Event; and
 - 15.1.4. if the period of delay or non-performance continues for more than 90 days, the Party not affected may terminate this Agreement in accordance with Clause **8.2.1**.

15.2. Any Party affected by a Force Majeure Event must inform the other Party when the Force Majeure Event has stopped and must do so within a reasonable timeframe.

16. Governing Law

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

17. Jurisdiction

Subject to Clauses **14.1** and **14.4** each Party irrevocably agrees 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 or its subject matter or formation (including non-contractual disputes or claims).

18. Entire Agreement

- 18.1. This Agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
- 18.2. Each Party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.
- 18.3. Each Party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in this Agreement.
- 18.4. Nothing in this Clause **18** shall limit or exclude any liability for fraud.

19. Amendments

No amendment or variation of this Agreement shall be effective unless it is in writing and signed by a duly authorised representative of each Party using the **Contract Variation Notice**.

20. Survivability.

All provisions of this Agreement relating to confidentiality, non-disclosure, intellectual property, disclaimers, limitation of liability, indemnification, and payment, and any other provisions which must survive in order to give effect to their meaning, shall survive the termination of this Agreement.

21. Signatures

IN WITNESS WHEREOF the Parties have executed this Agreement the day and year first above written as follows:

Signed for and on behalf of the Client.

Signed for and on behalf of the MSP.

Signature.....

Signature.....

Name.....

Name.....

Title.....

Title.....

Date.....

Date.....