MSP Services SOW v5 - 26 June 2026

STATEMENT OF WORK — MSP SERVICES

> ***Generic SOW v5 — 26 June 2026.*** *This Statement of Work (**"SOW"**) is a generic template used for every COR client purchasing MSP Services. It is entered into under and forms part of the **Master Services Agreement** (**"MSA"**) between **COR Solutions Services Limited** (the **"Supplier"** or **"COR"**) and the **Client** (as identified in the MSA and the Client Profile counter-signed under and alongside the MSA). In this SOW, the terms "COR" and "the Client" have the meanings given to them in the parties block of the MSA. Capitalised terms not otherwise defined here have the meanings given in the MSA. In the event of conflict between this SOW and the MSA, the SOW prevails for matters specifically addressed in this SOW (Services scope, charges, SLA, DPA, sub-processors), and the MSA prevails on all other matters. The Client's elected Services, units and SOW commencement date are set out in the **Client Profile**, and the applicable charges, applied Credits and elected payment frequency are set out in the **Pricing Agreement**, each issued under the MSA and counter-signed by the Client.*

SOW reference: `sow-msp-services-v3` (generic) **SOW commencement date**: as set out in the Client Profile **Minimum Term**: 12 months from the SOW commencement date (unless otherwise stated in the Client Profile)

---

1. Services covered

This SOW covers the following Services from COR's Services Catalogue (current Catalogue version applicable at signature: 2026-06-26):

Service	Service name	Trading brand
Service 1	MSP Remote IT Support	COR Solutions
Service 5	Office 365 Backup	COR Solutions
Service 6	Endpoint Detection and Response (EDR)	COR Solutions

Service	Service name	Trading brand
Service 7	Cloud-managed Endpoint Encryption *(optional — see Client Profile for election)*	COR Solutions
Service 8	Email Security and Phishing-Awareness Training	COR Solutions

---

2. SCHEDULE 1 — Services & Deliverables

Service 1 — MSP Remote IT Support

COR shall provide remote managed IT support to the Client's user devices and network endpoints, comprising:

- Endpoint health monitoring (hardware health, disk capacity, security events, patch compliance);
- Troubleshooting of supported Windows and macOS workstations;
- User account management within the Client's Microsoft 365 and/or Google Workspace tenants (joiners, leavers, password resets, group / sharing changes, multi-factor authentication);
- Setup of new devices and new users (booked via COR's online appointment booking platform);
- Printer setup and ongoing support for supported printers;
- Network device management (routers, switches, access points) for supported devices on the Client's premises;
- Security patching of supported operating systems and core applications under COR's management; and
- Response to support requests during Business Hours per Schedule 5 of this SOW.

Out of scope (chargeable separately or not provided):

- On-site / in-person attendance (available by separate arrangement at COR's day rate per MSA clause 5.3);
- Data recovery (not provided);
- Hardware repair (advisory only; physical repair by the manufacturer or a third-party engineer);
- Hardware or software procurement (procured by the Client unless separately agreed);
- Third-party software not on COR's supported list;
- Cyber-incident forensic investigation (separate engagement);
- **Local-device backup** of macOS or Windows workstation data outside the Microsoft 365 tenant (the Client is responsible for local-device backup, e.g. via an external USB drive or a separately-elected cloud backup service. Where the Client uses

OneDrive Known Folder Move for Desktop / Documents / Pictures, those folders sync into the M365 tenant and are covered by Service 5 (O365 Backup)); and

- **Microsoft Defender** is part of the Client's own Microsoft 365 licence and is the Client's own subscription — not a COR-provided service. Where present, Defender complements but does not replace Service 6 (EDR) or Service 8 (Email Security).

Setup of new devices and new users is included in the per-device Charge for this Service and is booked via COR's online appointment booking platform. Setup is normally offered on the next available Business Day subject to mutual availability.

Service 5 — Office 365 Backup

Daily backup of the Client's Microsoft 365 tenant via COR's elected M365 backup provider (the specific provider is identified in the Client Profile), comprising:

- **Exchange Online** mailboxes (email);
- **OneDrive for Business**;
- **SharePoint** sites; and
- (where supported by the backup provider) Microsoft Teams chat and files, Calendars and Contacts.

The provider may be subject to its own Fair Use Policy on storage; where this applies it is recorded in the Client Profile. The data residency of backups is recorded in the Client Profile.

Deployment mode: Automated tenant backup (default — all licensed M365 users in the Client's tenant are automatically included) unless the Client elects Manual setup in the Client Profile.

Data retention: backup retention is the period configured by COR for the Client (subject to the backup provider's policies). The specific retention configured for the Client is recorded in the Client Profile and may be varied by Change Order.

Restoration: COR provides restore services on a **reasonable-endeavours basis**. No specific restore time, recovery point or success rate is guaranteed. Restoration depends on the volume and nature of the data being restored and on the backup provider's performance under its own service standards.

Client obligations for this Service:

- Maintain administrative access for COR's backup integration to the Client's M365 tenant (Automated mode);
- Periodically verify backup integrity by requesting test restores (COR recommends quarterly verification).

Service 6 — Endpoint Detection and Response (EDR)

Endpoint detection and response on supported Client devices via COR's elected EDR platform (the specific platform is identified in the Client Profile), comprising:

- Endpoint anti-virus and anti-malware protection;
- Behavioural threat detection;
- Endpoint detection and response;
- Centralised management and alerting via COR's RMM platform (identified in the Client Profile);
- Security event monitoring and alert-driven response within the Service 1 SLA during Business Hours.

Out of scope: cyber-incident forensic investigation (separate engagement).

Service 7 — Cloud-managed Endpoint Encryption *(optional)*

Where elected by the Client in the Client Profile, COR provides cloud-managed endpoint volume encryption via COR's elected encryption platform (the specific platform is identified in the Client Profile), applied to supported Client devices on enrolment.

Service 8 — Email Security and Phishing-Awareness Training

Email security and phishing-awareness training via COR's elected platform (the specific platform is identified in the Client Profile), comprising:

Email security capabilities:

- Inbound and outbound email filtering;
- DLP (data loss prevention) filters;
- Attachment reputation service and sandboxing;
- URL defence;
- Emergency Inbox / Instant Replay (continuity in the event of mail-flow disruption — typically up to 30 days);
- Email encryption;
- Social-media account protection.

Phishing-awareness training:

- Simulated phishing and attachment campaigns (simulated-phishing campaigns);
- Library of security training modules covering email security, password protection, safer web browsing, data-entry phishing, physical security and related cybersecurity topics.

The specific feature set delivered depends on the email-security platform in use and the tier elected for the Client; both are recorded in the Client Profile.

Out of scope: forensic investigation of phishing incidents (separate engagement).

Data placement guidance (for the Client's safety)

COR's backup service (Service 5) protects the Client's **Microsoft 365 cloud data only**: email (Exchange Online mailboxes), OneDrive for Business, SharePoint, and (where supported by COR's backup platform) Microsoft Teams chat and files, Calendars and Contacts. Data that lives **only on a local device** (Mac or Windows workstation, external drives not synced to M365) is **not covered** by COR's backup.

COR therefore recommends, and the Client acknowledges, that:

- **Primary storage**: the Client should keep all work content in OneDrive for Business or SharePoint. The Client is recommended to enable Microsoft's OneDrive Known Folder Move (KFM) feature on managed devices, which redirects the Desktop, Documents and Pictures folders into OneDrive — these folders then sync automatically into the Microsoft 365 tenant and are covered by Service 5;
- **Local-only data**: where the Client chooses to hold data only on a local device (e.g. very large media files, locally-downloaded archives, application data outside the M365 tenant), the Client is responsible for periodic backup of that local data. A pragmatic baseline for a single-user workstation is an **external USB drive plugged in periodically** for a Mac Time Machine backup (or equivalent Windows backup). Where more comprehensive automated local-device cloud backup is required, this is available from COR as a separately-elected paid Service (chargeable under a Change Order); and
- **Mobile devices** (phones, tablets): COR's backup does not extend to local mobile-device storage beyond what syncs into M365. The Client should configure device-native backup (iCloud, Google Backup) for personal mobile-device data.

This guidance is operational and advisory; it does not vary the Services scope or pricing, but it makes clear what is and is not covered by COR's backup arrangements so the Client can plan its own data placement accordingly.

---

3. SCHEDULE 2 — Charges and Payment

Pricing is not contained in this SOW. Current List Rates, Standard Credits available, payment-frequency options and any Pete-agreed discounts applicable to the Client are set out in the **Pricing Agreement** issued by COR alongside the Client Profile and counter-signed by the Client.

Part A — Structural rules (apply regardless of current price level)

1. **Visible-value billing.** Where a Credit applies, it is shown as a separate line on each invoice — both the gross List Charge for the Service AND the Credit applied — so the Client always sees the value being given.

2. **Calculation each month.** COR determines the billable quantities (devices, users) for each Service in scope under this SOW each calendar month. The applicable List Rate (per the Pricing Agreement in force) is applied to the actual quantity. Any Credit (per the Pricing Agreement) is shown as a separate line on the invoice and reduces the net amount payable.
3. **Additions and removals** are rounded to the next full calendar month (added Services count from the start of the calendar month following addition; removed Services are removed from the start of the calendar month following the removal request).
4. **Service changes do not require contract amendment.** Adding, removing or changing the quantity of any Service is effected by COR re-issuing the Client Profile and (if the change affects what is being billed) the Pricing Agreement. No amendment of this SOW or the MSA is required.
5. **Annual price review.** COR may review the published List Rates and Standard Credits not more than once per 12-month period, per MSA clause 4.7. Updated pricing is issued by COR as a new Pricing Agreement with at least 30 days' written notice to the Client. The Client may discuss / object on reasonable grounds; failing agreement the Client may terminate the affected Services at the end of the then-current Minimum Term.
6. **Additional work outside the elected Services** is quoted by COR on a per-job basis and agreed in writing by the Client before COR commences the work (MSA clause 5.3).

Part B — Payment-frequency options (the menu)

The Client may elect, in the Pricing Agreement, any of the following payment frequencies:

- **Monthly Direct Debit** *(default)* — standard List Rate applies
- **Annual commitment billed monthly** — discount per the current Pricing Agreement
- **Annual paid upfront** — higher discount per the current Pricing Agreement

Changing the elected frequency (per MSA clause 5.2A): moves UP the commitment ladder (e.g. monthly to annual upfront) take effect from the next invoice cycle on reasonable written notice; moves DOWN the commitment ladder (e.g. annual upfront back to monthly) take effect only from the next SOW renewal date, so that any discount applied for a committed period is not undermined.

The **Client's elected payment frequency at signature**, and the resulting discount applied to the List Charges, are set out in the **Pricing Agreement**.

---

4. SCHEDULE 3 — Data Processing Agreement (UK GDPR Article 28) for the MSP Services

1. Processing details

Item	Description
Subject-matter	Processing of personal data on the Client's M365 tenant, managed devices and security platforms, in connection with provision of the MSP Services
Duration	From this SOW's commencement date through its Term and any continuation period, until deletion or return of personal data per section 11 below
Nature and purpose	Storage, monitoring, backup, security analysis, threat detection, in support of the MSP Services
Categories of personal data	Identifiers of Client's own staff and contractors (names, email addresses, contact information); communication content (email, chat, document content within the M365 tenant); access and security event logs; any personal data within Client's matter files held on the M365 tenant
Special-category data (UK GDPR Article 9)	Where the Client's regulated status (set out in the Client Profile) or sector means the Client's M365 tenant may include special-category personal data (UK GDPR Article 9) or information held under duties of confidence to third parties (including, where applicable, legal professional privilege, medical confidence, financial confidence or analogous obligations), the Parties acknowledge that COR's role is limited to providing the Services and does not include substantive processing of such content save where strictly necessary per MSA clause 7.3.
Categories of data subjects	The Client's staff and contractors; third parties whose data is held by the Client in the M365 tenant; any further categories noted in the Client Profile.

2. Controller and Processor

The Client is the Controller; COR is the Processor.

3. Controller's instructions

COR shall process personal data only on documented written instructions from the Client (which may be standing instructions reflected in this SOW), except where required to do so by applicable law.

4. Security measures

COR shall implement and maintain appropriate technical and organisational measures appropriate to the risk under UK GDPR Article 32, having particular regard to the sensitivity of the Client's matter data. These measures include:

- (a) encryption in transit (TLS 1.2 or later for all managed services);

- (b) encryption at rest on backup and storage Sub-processors;
- (c) access control, role-based access management and multi-factor authentication for COR personnel;
- (d) backup and fixity-check cadence per Schedule 5;
- (e) endpoint protection via Service 6;
- (f) email security via Service 8;
- (g) secure logging and monitoring; and
- (h) UK / EU region pinning for personal-data-bearing Sub-processors where the Sub-processor offers this option.

5. Confidentiality of personnel

COR shall ensure that all personnel authorised to access the Client's personal data have committed themselves to confidentiality. Where the Client Profile flags the Client as subject to specific duties of confidence (legal professional privilege, medical confidence, financial confidence or analogous obligations), COR personnel handling Client data are briefed accordingly.

6. Sub-processors

COR may engage the Sub-processors listed in **Schedule 4** of this SOW, which the Client authorises. Sub-processor change notice procedure per MSA clause 7.5.

7. Assistance with data subject rights

COR shall, taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as possible, in fulfilling its obligation to respond to requests for exercising data-subject rights. COR shall acknowledge such assistance requests within 5 Business Days.

8. Assistance with Controller's UK GDPR obligations

COR shall assist the Client in ensuring compliance with its obligations under UK GDPR Articles 32 to 36, taking into account the nature of the processing and the information available to COR.

9. Personal data breach

COR shall notify the Client without undue delay (and in any event within 48 hours) after becoming aware of a personal data breach affecting personal data processed under this Schedule. Notification shall describe the nature of the breach, categories and approximate numbers of data subjects and records affected, likely consequences, and measures taken or proposed.

10. Audit

COR shall make available to the Client information necessary to demonstrate compliance with this Schedule, and allow audits by the Client or a Client-mandated auditor. Audits limited to once per calendar year (save in the event of a personal data breach), on reasonable written notice and at the Client's cost. SOC 2 Type 2 or equivalent reports from Sub-processors may be accepted in lieu of direct audit.

11. Return or deletion at end

On termination of this SOW (or earlier on the Client's written request), COR shall, at the Client's option, return all personal data processed under this Schedule or destroy it (and certify destruction), save for any retention required by applicable law or for COR's own records (limited and proportionate).

12. International transfers

Personal-data-bearing processing operations shall be carried out in the United Kingdom or European Economic Area unless otherwise agreed in writing or required for the specific Sub-processor (notably, the storage region of the M365 backup provider in use). Any future Sub-processor or change requiring an international restricted transfer shall be accompanied by the UK Addendum to the EU SCCs (ICO version, March 2022) or any successor mechanism.

13. Regulated-client operational protection (where Client is flagged as regulated in the Client Profile)

Where the Client Profile flags the Client as regulated (SRA, FCA, GMC, ICO or any other regulator), and accordingly subject to specific confidentiality duties owed by the Client to its own third parties, COR shall not — save in providing the Services and at the Client's reasonable direction — access, monitor, copy, transfer or analyse the substantive content of any third-party information held in the Client's M365 tenant. Any incidental access by COR personnel in the course of providing technical support shall be treated as held under a duty of confidence equivalent to that owed by the Client to its own third parties. This section 13 operates as an operational complement to MSA clauses 7.3 and 10.2 (which carry the generic position).

---

5. SCHEDULE 4 — Sub-processors

This Schedule reflects the Sub-processors in use as at the date of this SOW. COR may add, replace or remove Sub-processors per MSA clause 7.5 (notice → objection right → suspension / termination). When a Sub-processor changes, COR re-issues this Schedule — no amendment of this SOW or the MSA is required. Superseded Sub-processor Schedules are retained for audit history.

Sub-processor role (category)	What it does	Region (typical)
PSA + RMM + remote-access platform	Ticketing, billing, audit log, remote monitoring and management of supported endpoints, remote-access for end-user support	UK / EU where personal-data-bearing
Microsoft Corporation	Where the Client uses Microsoft 365 — Client's own tenant; COR has admin access only as Processor on the Client's behalf	Per the Client's M365 configuration
Google LLC	Where the Client uses Google Workspace — Client's own tenant; COR has admin access only	Per the Client's Google Workspace configuration
EDR provider	Endpoint detection and response platform (Service 6)	EU / UK typical
Cloud encryption provider	Cloud-managed endpoint encryption (Service 7, where elected)	EU / UK typical
Microsoft 365 backup provider	Backup of the Client's M365 tenant (Service 5); subject to that provider's Fair Use Policy where applicable	EU / UK typical
Email security and phishing-awareness training provider	Email filtering, DLP, attachment defence, URL defence, security-awareness training (Service 8)	EU / US per the provider's regional configuration

The actual sub-processors engaged for the Client at the date of this SOW (including specific product names, plan tiers and data residency) are listed in the **Client Profile**. Where the actual sub-processor for any category changes during the Term, the change is notified per MSA clause 7.5 and reflected in a re-issued Client Profile.

Sub-processor changes follow the notice procedure in MSA clause 7.5 and Schedule 3 clause 6 of this SOW.

---

6. SCHEDULE 5 — Support and Service Levels

Support request channels

The Client may request support by:

- emailing the dedicated COR support mailbox (address notified to the Client at SOW commencement); or
- leaving a voicemail message on the dedicated COR voicemail line (number notified to the Client at SOW commencement).

Support requests are tracked as tickets in **COR's PSA platform** (the specific platform is identified in the Client Profile) with status, audit trail and operational continuity. Setup tasks (new device provisioning, new user account creation, significant device reconfiguration) are booked via COR's online appointment booking platform (link notified to the Client at SOW commencement).

Support SLA

Support requests received **during Business Hours** (09:00–17:00 Monday to Friday, excluding England and Wales public holidays) shall be:

- (a) acknowledged by COR; AND
- (b) the subject of COR's commencement of first-attempt remediation;

within **4 Business Hours of receipt**. Time to resolution depends on the nature and complexity of the request and is on a reasonable-endeavours basis.

Support requests received outside Business Hours are queued and treated as received at the start of the next Business Day.

Setup SLA

Setup requests (new device, new user, significant reconfiguration) are booked via COR's online appointment booking platform. COR uses reasonable endeavours to offer the next available Business Day where possible. Setup work is included in the per-device Charge under Service 1 and is not subject to the 4-Business-Hour Support SLA.

Backup, EDR and Email Security service standards

- **Service 5 (O365 Backup)**: daily Microsoft 365 backup via the M365 backup provider; restoration on reasonable-endeavours basis; quarterly Client-initiated test restore recommended;
- **Service 6 (EDR)**: 24/7 platform monitoring; alert-driven response within the Service 1 SLA during Business Hours;
- **Service 8 (Email Security)**: 24/7 platform; alert-driven response within the Service 1 SLA during Business Hours.

Patching cadence

Security patching follows the recommended patch-cadence guidance issued by COR's RMM platform (identified in the Client Profile) for supported operating systems and core applications managed under COR's RMM. Updates to the RMM platform's published guidance are followed by COR.

---

7. SCHEDULE 6 — Change Control Procedure for this SOW

1. Either Party identifies a need for a change and sends a written request.

2. Where the change is the addition or removal of a Service or change in quantity (devices, users), Part B of Schedule 2 of this SOW is updated by email exchange between the Parties; the change takes effect from the next calendar month.
3. Where the change is substantive additional work outside the elected Services, the Parties may either (a) enter a separate SOW under the MSA, or (b) where the work is minor, agree it as additional work under this SOW. Charges for additional work are quoted by COR in writing on a per-job basis and agreed in writing by the Client before COR commences the work (per MSA clause 5.3).
4. COR is not obliged to commence chargeable additional work until the change is agreed in writing.

---

8. Execution by incorporation

This Statement of Work is incorporated by reference into the **Client Profile** counter-signed by the Parties on or about the SOW commencement date set out in the Client Profile. The Parties' agreement to and acceptance of this SOW is **evidenced by their signatures on that Client Profile** (per MSA clauses 14.8 and 14.9). No separate signature is required on this SOW.

End of SOW.