

MANAGED SERVICES AGREEMENT (MSA)

Between:

ACS Technology Group Ltd ("Provider" or "ACS")

Kismet Buildings, Otley Road, Baildon, West Yorkshire, BD17 7HB

And:

[Client Legal Name] ("Client")

Effective Date: [DD Month YYYY]

Initial Term: [12 / 24 / 36 Months]

Renewal: Auto-renews for 12-month periods unless terminated under Section 14.

1. EXECUTIVE SUMMARY

ACS delivers a comprehensive Managed IT Service encompassing proactive monitoring, patching, cybersecurity operations, IT support, infrastructure management, cloud administration, and strategic IT leadership.

This Agreement sets out:

- The services ACS will deliver
- The boundaries, SLAs, and responsibilities
- Legal, commercial and compliance terms
- Optional solution areas available via Statement of Work (SOW)

2. DEFINITIONS

Key terms include:

Agreement, Services, SLA, Incident, Service Request, Maintenance, Confidential Information, Personal Data, Data Protection Laws, Change Request, Fees, Term, Service Credits, Excluded Services, Deliverables, Force Majeure, Controller, Processor, Sub-processor, SOW (Statement of Work).

3. SCOPE OF MANAGED SERVICES

ACS provides the services in Schedule A, including:

3.1 Service Desk

- UK-based Helpdesk (09:00–18:00, Mon–Fri)
- Multi-tier triage and escalation
- Ticket lifecycle management and reporting

3.2 Proactive Monitoring & Maintenance

- Monitoring across endpoints, servers, cloud & network
- Automated remediation where appropriate
- OS and application patching
- Fault alerting and trend analysis

3.3 Cyber Security Services

- Endpoint protection (AV/EDR)
- Identity security (MFA, Conditional Access)
- Managed Detection and Response (MDR)
- Threat monitoring and alert handling
- Baselines and hardening
- Security advisory
- Malware response assistance

3.4 Microsoft 365 & Azure Services

- Tenant administration
- Licence optimisation and audits
- User onboarding/offboarding
- SharePoint/Teams governance
- Conditional Access and identity controls

3.5 Backup & Disaster Recovery

- M365 backup
- Server image backup
- Retention governance
- Restore testing
- DR readiness guidance

3.6 Network & Infrastructure Management

- Firewall, switching, wireless
- Firmware updates and hardening
- Performance optimisation
- Connectivity troubleshooting

3.7 Strategic Technology Partnership

- Quarterly Business Reviews
- Roadmaps
- Cyber posture reviews
- Licensing, usage, and optimisation reporting

3.8 Repair Services (Top-Level – Per SOW)

ACS may deliver repair services for supported devices as scoped in a specific SOW:

- Device triage and assessment
- Repair/refurbishment workflow
- Logistics, courier handling and RMA
- Parts replacement
- Chain-of-custody processes
- Sanitisation (software wipes if required)

Note: All SLAs, pricing tiers, device catalogues and conditions are defined per SOW.

3.9 Hardware Procurement Services (Per SOW)

ACS may provide:

- Supply of desktops, laptops, servers, networking, peripherals
- Pre-staging, imaging, configuration
- Asset tagging, inventory and lifecycle planning
- Warranty coordination and vendor escalation
- Bulk refresh projects

All volumes, models, warranties, lead times and service deliverables defined per SOW.

3.10 AV Deployment Services (Per SOW)

ACS may design and implement AV/meeting room environments:

- Teams Rooms / Googlemeet Rooms
- Display installation and mounting
- Audio systems and structured cabling
- Collaboration equipment
- Commissioning and user training

Specifications, schematics and room-by-room deliverables defined per SOW.

3.11 Software Solutions & Deployment (Per SOW)

ACS can deliver software solutions such as:

- M365, Adobe and SaaS rollout
- Security tools (EDR/MDR, Compliance Suite, CA rules)
- Azure and hybrid cloud applications
- Application packaging & automated deployment
- CRM/ERP or vertical-market solutions (where supported)

Scope, licensing, rollout schedule and acceptance criteria defined per SOW.

3.12 Managed Print Solutions (Per SOW)

Services may include:

- Print fleet assessment
- Device supply and installation
- Print management software (Papercut etc.)
- Toner logistics and automated replenishment
- Usage reporting and optimisation
- Break-fix response (via certified partners)

All SLAs, page volumes, device lists and consumable terms are defined per SOW.

3.13 Telecoms & Connectivity Solutions (Per SOW)

ACS may provide:

- Cloud telephony (VoIP)

- Microsoft Teams Calling enablement
- SIP Trunks and number porting
- Broadband, leased line, SD-WAN
- Telephony infrastructure and call-flow design
- Mobile Sim Deployment and Management

Connectivity speeds, installation windows and SLAs defined per SOW.

3.14 Additional Services via SOW

Beyond this Agreement, ACS may deliver:

- Cloud migrations
- Cybersecurity assessments
- Identity restructuring
- Office relocations / technology fit-outs
- Large-scale infrastructure refresh
- Data analytics / BI solutions

Any additional service is only binding once an SOW is signed.

3.15 Excluded Services

Unless specifically included by SOW:

- Cabling & electrical work
 - Obsolete/unsupported systems
 - Software development
 - Incidents caused by security controls being bypassed
-

4. ONBOARDING & TRANSITION

- Discovery & audit
- Tooling deployment
- Documentation
- Security baseline review
- Go-Live

- Hypercare period
- Transition into BAU

(Full detail in Schedule C.)

5. FEES & PAYMENT

- MRR invoiced monthly in advance
 - Licensing invoiced monthly
 - Project/SOW work billed separately
 - 30-day payment terms
 - Automatic vendor cost pass-through
-

6. SLAs (Service Level Agreement)

Response Times:

- P1 Critical: 1 hour
- P2 Major: 4 hours
- P3 Standard: 8 hours
- P4 Low: Next Business Day

Resolution: Best-endeavours depending on complexity.

Maintenance: 72 hours' notice where practicable.

Service Credits (Optional): Defined per client.

(Full matrix in Schedule B.)

7. CHANGE CONTROL

All scope changes follow ACS's formal Change Request process.

8. CLIENT RESPONSIBILITIES

Client must:

- Provide access, credentials, accurate data
- Maintain valid third-party licences
- Notify ACS of changes affecting IT
- Provide adequate connectivity infrastructure

- Avoid bypassing or disabling security controls
-

9. ACS RESPONSIBILITIES

ACS will:

- Deliver all contracted services
- Maintain documentation and security controls
- Apply updates and patches
- Provide support and escalation
- Deliver quarterly reporting and recommendations

Any changes can be agreed by both parties via an additional SOW

10. SECURITY & DATA PROTECTION

- UK GDPR & DPA 2018 apply
 - Data Processing Addendum included in Schedule E
 - 72-hour Data Incident notification
 - Sub-processors used only with safeguards
 - Data stored securely; deleted upon termination
 - ACS maintains an ISO-aligned management system, including ISO 9001 and ISO 27001 certifications, and ISO 22301 where applicable, to ensure consistent quality, security, and business continuity across all services.
 - ACS ensures that all approved Subprocessors operate under security and operational standards equivalent to ACS's own ISO-aligned management system.
-

11. CONFIDENTIALITY & PUBLICITY

- Mutual confidentiality
 - No external disclosure without written approval
-

12. INTELLECTUAL PROPERTY

- Pre-existing IP remains with each party
- ACS retains ownership of scripts, tooling, templates
- Client receives a non-transferable licence to use deliverables internally

13. WARRANTIES & DISCLAIMERS

- ACS guarantees reasonable skill and care
- ACS does not guarantee third-party platform uptime
- No implied warranties apply

14. INDEMNITIES

- ACS indemnifies Client for IP infringement arising from ACS deliverables
- Client indemnifies ACS for misuse of systems, unlawful data, or unsupported configurations

15. SUSPENSION OF SERVICE

ACS may suspend if:

- Fees overdue
- Security risks present
- Client blocks required access
- Material breach occurs

16. TERM, TERMINATION & EXIT

- 30-day remedy period for breach
- Early termination charges apply if Client ends early

17. LIABILITY

- Liability capped at 12 months of Fees
- No liability for indirect losses
- Exceptions: death/injury, fraud, wilful misconduct

18. FORCE MAJEURE

Events beyond reasonable control (weather, strikes, pandemics, cyberattacks, utility failures, vendor outages).

19. DISPUTE RESOLUTION

Escalation → mediation → legal action (England & Wales).

20. ORDER OF PRECEDENCE

1. Signed SOW
 2. This Agreement
 3. Change Requests
 4. Data Processing Addendum
 5. Schedules
 6. Proposal documents
-

SCHEDULE A — SERVICE DESCRIPTION

(Including Hardware, AV, Software, Managed Print, Telecoms & Repair Services — all per SOW)

SCHEDULE B — SLA MATRIX

B1. Core Support Hours

ACS provides support during the following hours unless otherwise agreed:

- **Monday–Friday:** 09:00 – 18:00UK time
 - **Excluding** UK public/bank holidays
 - Out-of-hours support available **per SOW**
-

B2. Priority Definitions & Examples

Priority	Definition	Examples
P1 Critical	Full service outage, business-critical failure, widespread impact	Entire site offline, server offline, major security breach, critical app unavailable
P2 Major	Multi-user degradation or outage	CRM slowdown, shared drive inaccessible, network instability
P3 Standard	Single-user impact or moderate disruption	Printing issues, application errors, password resets

Priority	Definition	Examples
P4 Low	Non-urgent requests or administrative tasks	New user setup, mailbox changes, permission adjustments

B3. Response & Update Targets

Priority	Response Time	Update Frequency
P1	1 hour	Every 2 hours
P2	4 hours	Every 4 hours
P3	8 hours	End of Business Day
P4	Next Business Day	As required

Response = ACS begins active work on the issue.

Resolution = Best-endeavours based on complexity, vendor dependencies, and approvals.

B4. Resolution Targets

ACS operates on a **best-endeavours** basis for all resolutions.

Resolution depends on:

- Vendor escalations (Microsoft, hardware OEMs, ISPs)
- Access provided by Client
- Complexity, third-party issues, or required change approvals

ACS will always endeavour to provide immediate workarounds where full resolution is delayed.

B5. Escalation Process

1. **Level 1:** Support Desk Engineer
2. **Level 2:** Senior Engineer
3. **Level 3:** Infrastructure / Cloud / Security Specialist
4. **Level 4:** Head of MSP
5. **Level 5:** Director escalation

Escalation is automatic for P1 and P2 incidents.

B6. Scheduled & Emergency Maintenance

- Planned maintenance requires **72 hours' notice** where practicable.
 - Emergency maintenance may be performed immediately to protect security or service continuity.
 - ACS will notify the Client at the earliest safe opportunity.
-
-

B7. SLA Exclusions

The SLA does not apply where:

- Client infrastructure is unsupported or end-of-life
 - Client has prevented access or disabled required tooling
 - Internet, power, or third-party vendor failures occur
 - Client changes systems without notifying ACS
 - Force Majeure events occur
 - Issues arise from third-party unmanaged apps
-

SCHEDULE C — ONBOARDING WORKFLOW

C1. Discovery & Technical Audit

ACS completes a full audit including:

- Network architecture
- Server/storage infrastructure
- Security posture
- Microsoft 365/Azure environment
- Endpoint estate
- Telecoms & connectivity review (if included)
- Managed Print environment (if included)

Deliverables:

- Asset inventory
- Network diagrams
- Security baseline assessment

C2. Tooling Deployment

ACS deploys:

- RMM agent
- AV/EDR agent
- Monitoring integrations
- Backup and DR validation
- Administrative access configuration

Client must provide:

- Required credentials
 - Administrative access pathways
 - Site access (if required)
-

C3. Documentation Migration

ACS builds or updates:

- Configuration records
 - Access & credentials vault
 - Network diagrams
 - Backup/DR plans
 - Application/line-of-business mappings
 - User lists & licensing map
-

C4. Go-Live Procedure

- Communications sent to Client teams
 - Support channels opened
 - Logging and SLA tracking activated
 - All priority systems onboarded
 - Service Desk introduced to stakeholders
-

C5. Hypercare Phase (First 30 Days)

- Enhanced monitoring
 - Trend analysis
 - Issue backlog clearing
 - Stabilisation of systems
 - Additional end-user support as needed
 - Weekly check-ins with Client
-

C6. Transition to ACS

- Handover to ongoing support model
 - Final onboarding review meeting
 - Documentation added to ACS Secure Site
 - Quarterly Business Review cycle initiated
-

SCHEDULE D — PRICING

D1. Monthly Recurring Revenue (MRR)

- Managed Services (per user / per device / per site)
- Monitoring & Patching
- Cyber Security licence bundles
- Backup & DR services
- Cloud management fee
- Network management fee

Pricing examples (illustrative only):

- Per user managed service
 - Per server fee
 - Per network device
 - Per site uplift
-

D2. Licensing

Licences billed monthly based on:

- Microsoft CSP consumption
- Security tools (EDR, MFA, CA enforcement tools)
- Backup licensing
- Cloud consumption estimates (Azure)

ACS provides:

- Monthly licensing reconciliation
- Usage & optimisation reporting
- Licence right-sizing recommendations

Pricing Schedule can be changed to different billing periods dependent on product or client and ACS requirement but will be an additional contract.

D3. Professional Services / Project Fees

Professional services billed per:

- **Fixed price** (for scoped projects)
- **Time & materials** (T&M hourly or daily rate)

Rate card may include:

- Support Engineer
- Senior Engineer
- Network/Security Specialist
- Cloud Architect
- Project Manager

D4. Travel, Onsite & Out-of-Hours

- Standard onsite rate per engineer
- Out-of-hours rate (evenings/weekends)
- Emergency onsite callout rate

D5. Indexation & Price Adjustments

- Annual CPI
- Vendor cost passthrough

- Mid-year cloud licensing changes
-

D6. Payment Terms

- 30 days net
 - Direct debit required unless agreed otherwise
-

SCHEDULE E — DATA PROCESSING ADDENDUM

E1. Roles

- **Client** = Data Controller
- **ACS** = Data Processor

ACS processes data **only on documented instruction from the Client.**

E2. Nature & Purpose of Processing

ACS processes Personal Data to:

- Deliver Managed Services and support
 - Provide cloud and infrastructure management
 - Administer user accounts and permissions
 - Provide secure backup and restoration
 - Fulfil SOW-based project activities
 - Maintain documentation
-

E3. Categories of Data Subjects

- Client employees
 - Client contractors
 - Client customers (if applicable to service)
 - IT service accounts
-

E4. Categories of Personal Data

- Contact details

- Account identifiers
- Email & collaboration data (M365)
- System access logs
- Backup data stores
- Support ticket data

ACS does **not** process special category data unless explicitly agreed in an SOW.

E5. Data Security Measures

ACS maintains technical and organisational controls including:

- Encryption at rest/in transit where applicable
- MFA-protected admin access
- Endpoint and cloud security controls
- Network segmentation
- Backup integrity checks
- Logging & auditing
- ISO-aligned internal governance

ACS reviews security measures annually.

E6. Sub-processors

ACS may use approved Sub-processors such as:

- Microsoft (Azure, M365)
- Datto / Acronis / backup vendors
- RMM/EDR vendors
- Telecoms carriers (if applicable)

ACS will:

- Maintain a Sub-processor list
 - Notify Client of changes with reasonable notice
-

E7. Data Incident Notification

ACS will notify the Client:

- **Without undue delay**, and
- **Within 72 hours** of becoming aware of a Data Incident

Notification will include:

- Nature of incident
 - Categories of data affected
 - Approximate volume
 - Likely consequences
 - Mitigation actions taken
-

E8. International Transfers

Where data is transferred outside the UK:

- Approved transfer mechanisms will be used
 - Standard Contractual Clauses (SCCs) applied where required
 - Data transfer risk assessments performed where necessary
-

E9. Data Retention & Deletion

Upon termination or Client request:

- ACS will delete or return all Personal Data
 - Backups will be securely purged after the retention expiry period
 - Documentation and access vault entries will be destroyed securely
-

E10. Audit Rights

Client may audit ACS's compliance:

- Once per 12-month period
- With reasonable notice
- During business hours
- Without disruption to ACS operations

External audits are chargeable at ACS's standard professional rates.

E11. Liability under the DPA

Liability is governed by the main Agreement except where prohibited by law.

END OF AGREEMENT

