



## SERVICE DEFINITION DOCUMENT: IT SERVICES

---

### 1. SERVICE DESCRIPTION & SCOPE

Astaris will provide comprehensive, proactive IT management and support services, utilising a Remote Monitoring & Management (RMM) toolset to ensure a secure, reliable, and high-performance IT environment. The service encompasses end-user support, device management, network security, operational networking, and data management.

#### 1.1 SCOPE OF SERVICES

| Area                      | Description of Service Provided by Astaris                                                                 |
|---------------------------|------------------------------------------------------------------------------------------------------------|
| End User Services         | Provision of support channels, incident management, and user guidance.                                     |
| Device Management         | Monitoring, patching, security updates, asset management for computers/handhelds.                          |
| Security Management       | Deployment/management of anti-virus, content filtering, secure access controls.                            |
| Operational Management    | Network device monitoring (firewalls, switches, WAPs, printers), configuration management, change logging. |
| Application & Data Mgt.   | Management/monitoring of Office 365 environment, data backup, database maintenance.                        |
| Third-Party Software Mgt. | Triage, diagnosis, and escalation/ownership of issues with third-party vendors.                            |
| Account Management        | Scheduled reviews, "walk the floor" visits, performance monitoring, reporting.                             |

## **2. SERVICES**

### **2.1 END POINT MANAGEMENT**

#### **NINJA BACKUP**

Astaris utilises NinjaOne Data Protection to deliver a unified, cloud-native backup and disaster recovery service to our clients. Through our centralised management dashboard, we provide comprehensive data security across your entire infrastructure—from Windows and macOS endpoints to physical servers and virtual machines. Our managed service extends this protection to your critical SaaS environments, including Microsoft 365 and Google Workspace, ensuring your organisation's data is secure, compliant, and rapidly recoverable from a single, streamlined interface.

#### **NINJA MOBILE DEVICE MANAGEMENT**

NinjaOne Mobile Device Management (MDM) offers our clients a truly unified approach to endpoint security. By integrating this module into our core management platform, we can secure and monitor your mobile fleet—including iOS, iPadOS, and Android—right alongside your traditional Windows, macOS, and Linux infrastructure. This gives our team a "single pane of glass" view to ensure that every device in your organisation, whether a smartphone in the field or a server in the office, is protected, compliant, and performing optimally.

#### **SENTINEL ONE**

SentinelOne provides AI-driven, autonomous protection that neutralises advanced threats like ransomware in real-time. Our managed service secures your entire estate—endpoints, cloud workloads, and identities—using "Storyline" technology for instant event context and rapid response. Critically, we employ SentinelOne's one-click rollback to instantly restore files and ensure business continuity, providing industry-leading automation backed by our 24/7 technical oversight.

#### **CISCO UMBRELLA**

Astaris uses Cisco Umbrella as your first line of defense, automatically blocking dangerous websites and cyberattacks before they ever reach your devices. We provide this security for your entire team, whether they are in the office or working remotely, without the hassle of a slow VPN. By using world-class threat intelligence, Astaris keeps your internet connection safe and gives you a clear view of any unauthorised apps being used, ensuring your business stays protected from modern online risks.

## MICROSOFT INTUNE

Astaris uses Microsoft Intune to deliver a secure, modern workplace with these key benefits:

- Unified Management: We manage Windows, macOS, iOS, and Android from a single dashboard, ensuring consistent security and updates across all devices.
- Zero Trust Security: Automated "Compliance Policies" block non-compliant or outdated devices from accessing corporate data until they are secured.
- Secure BYOD: We protect business apps on personal phones without accessing private data, preventing sensitive information from being copied to personal apps.
- Zero-Touch Deployment: Using Autopilot, Astaris ships devices directly to users for automated over-the-air setup, eliminating manual IT imaging.
- Rapid Data Protection: We can remotely wipe corporate data from lost or decommissioned devices instantly while leaving personal files untouched.
- Cost Efficiency: This cloud-native approach removes the need for on-premises servers and complex VPNs, reducing overhead and improving connection speeds.

## MICROSOFT TEAMS

Microsoft Teams Essentials, a cost-effective, standalone collaboration platform for smaller organisations that avoids the need for full Microsoft 365 suites. Our managed service provides 30-hour meeting limits for up to 300 participants, 10GB of secure cloud storage per user, and full integration with your professional business domain. By leveraging Astaris to handle the setup and security, your team gains a professional identity with advanced tools for chat, file sharing, and hybrid collaboration, all backed by our expert 24/7 support.

## MANAGED IT SUPPORT PACKAGES

Astaris provides proactive IT support by shifting from the traditional "break-fix" model to a strategy focused on prevention and continuous optimisation. Our proactive approach ensures your infrastructure remains stable, secure, and high-performing.

### HOW ASTARIS DELIVERS PROACTIVE SUPPORT:

- **24/7 Real-Time Monitoring:** We use advanced RMM (Remote Monitoring and Management) tools to track the health of your servers, endpoints, and cloud services. We often identify and resolve hardware failures or software glitches before your staff even notices a problem.
- **Automated Patch Management:** Astaris automates the deployment of critical security updates and patches across all devices (Windows, macOS, and Linux). This ensures your systems are never left vulnerable to known exploits.
- **Predictive Maintenance:** By analysing system trends—such as failing hard drives or unusual CPU spikes—our team intervenes early to replace hardware or optimise software, preventing costly emergency downtime.
- **Managed Security Oversight:** We don't wait for a breach; we proactively hunt for threats using SentinelOne AI and Cisco Umbrella. We continuously refine your security policies to block emerging cyber threats at the source.
- **Strategic IT Reviews:** Astaris conducts regular "Technology Alignment" reviews. We look at your current setup against industry best practices to ensure your IT strategy evolves with your business goals, rather than just reacting to them.

### THE BUSINESS BENEFIT

By choosing Astaris for proactive support, you move away from disruptive IT emergencies toward a predictable, "always-on" environment. This increases staff productivity, strengthens your security posture, and allows your organisation to focus on its core mission while we handle the technical resilience

### GOOGLE WORKSPACE / MICROSOFT OFFICE 365

Astaris provides a fully managed service for Microsoft 365 and Google Workspace, delivering a secure and resilient email infrastructure through seamless, zero-downtime migrations of all historical data. We protect your organisation with enterprise-grade security, including Multi-Factor Authentication (MFA) and Data Loss Prevention (DLP), while simplifying access through Single Sign-On (SSO) via Microsoft Entra or Google Identity. By bolstering standard filters with AI-driven threat defense from Mimecast or Cisco Umbrella and ensuring long-term recovery with NinjaOne cloud-to-cloud backups, Astaris guarantees that your communication environment remains professional, compliant, and always protected against data loss

## EMAIL MIGRATION

Astaris employs a rigorous, multi-stage migration framework to ensure your transition to a new cloud email environment is seamless, secure, and completed with zero fuss.

The Astaris Staged Migration Workflow:

- **Credential Verification:** Our engineers first validate access permissions at both the source and destination environments. This step ensures a secure, authenticated connection is established before any data transfer begins.
- **Trial Migration:** We perform a limited test migration of select mailbox data to verify the project configuration. This phase identifies potential mapping issues early, ensuring the migration path is fully optimised.
- **Pre-Stage Migration:** To minimise the final switchover time, we pre-fill your new destination mailboxes with historical data (typically items older than 3 months). This background process allows your team to continue working on their current system without interruption.
- **Full Migration & MX switchover:** At the scheduled "Go-Live" moment, we redirect your MX records to the new mail server. We then execute the final migration pass to synchronise the remaining 90 days of data, ensuring no messages are lost during the transition.
- **Error Remediation:** Following the switchover, we perform a targeted "Retry Errors" pass. This process identifies and remigrates any specific items that initially failed, ensuring 100% data integrity without duplicating successfully moved content.

By utilising this proactive, phased approach, Astaris guarantees a professional and resilient migration to your new platform, supported by our 24/7 technical oversight.

## KNOWBE4 PHISHING SOFTWARE

KnowBe4 is training software that transforms your staff into a powerful "human firewall" through AI-driven education and real world simulations. Our service leverages Artificial Intelligence Defense Agents (AIDA) to personalise training based on individual risk, combined with automated phishing tests that typically reduce user vulnerability from 30% to under 5% annually. We provide immediate SecurityCoach feedback for risky behaviors and manage Compliance Plus to meet legal standards like GDPR. With Astaris, you receive data-driven reporting and Virtual Risk Officer insights, ensuring your security culture is measurable, compliant, and robust against modern social engineering.

## MIMECAST

Mimecast as an AI-powered safety net for your business communications, automatically blocking advanced threats like phishing, ransomware, and impersonation attacks. Beyond just email, this system secures collaboration tools like Microsoft Teams and provides a secure, long-term archive for your data. Our managed Mimecast service ensures your digital workspace stays protected and compliant under our 24/7 expert oversight.

## HOSTED VoIP TELEPHONY

Astaris provides a fully managed, cloud-based VoIP (Voice over IP) telephony service that replaces expensive, outdated on-premises phone systems. Our solution allows your team to make and receive professional business calls from any device—laptop, smartphone, or desk phone—ensuring your office is truly mobile.

### The Astaris Managed VoIP Advantage

- **Professional Features:** We configure your system with essential business tools, including Auto-Attendants (virtual receptionists), intelligent Call Queues, and voicemail-to-email, ensuring you never miss a client call.
- **Seamless Microsoft Teams Integration:** Astaris can turn your existing Microsoft Teams environment into a full business phone system, allowing your staff to manage meetings and external phone calls within a single, familiar app.
- **Significant Cost Savings:** By moving to the cloud, you eliminate traditional line rentals and hardware maintenance costs. Our flexible "per-user" pricing model ensures you only pay for what you actually use.
- **Rapid Deployment & Porting:** Astaris handles the entire setup, including the seamless transfer (porting) of your existing phone numbers, so there is no disruption to your business identity.
- **Global Reliability:** Our VoIP infrastructure is designed for high availability, ensuring crystal-clear call quality and a reliable connection regardless of where your staff are working.
- **End-to-End Call Centre Set Up:** Astaris provides a comprehensive, end-to-end VoIP call centre setup service, transforming your telephony into a modern, cloud-based Contact Centre with advanced queue management, omnichannel integration, CRM & tool integration, supervisor and reporting tools giving your managers the data needed to monitor agent performance, call volumes and SLA's.

## BENEFITS OF HOSTED VOIP

- |                                                           |                                  |
|-----------------------------------------------------------|----------------------------------|
| ✓ 4000 MINUTES TO UK LANDLINES & MOST UK MOBILES INCLUDED | ✓ OUT OF HOURS SERVICE           |
| ✓ DO NOT DISTURB                                          | ✓ IVR (PRESS 1 FOR... 2 FOR...)  |
| ✓ CALL TRANSFER                                           | ✓ VOICEMAIL                      |
| ✓ UNLIMITED HELP DESK SUPPORT                             | ✓ GREAT VOICE QUALITY            |
| ✓ MUSIC ON HOLD                                           | ✓ SAVE MONEY                     |
| ✓ CALL RECORDING                                          | ✓ MANAGE YOUR OWN CALLS          |
| ✓ CALL WAITING                                            | ✓ FLEXIBILITY FOR REMOTE WORKING |
| ✓ CALL QUEUING                                            | ✓ REALLY SIMPLE TO USE           |

## CONNECTIVITY

Astaris provides a fully managed service for procuring and managing high-speed internet connectivity, including leased lines, FTTP (Fibre to the Premises), and broadband services.

We act as a single point of contact, eliminating the need for you to manage multiple Internet Service Providers (ISPs) or deal with the complexities of "last-mile" support.

- **Connectivity Options:** Astaris provisions a range of options based on your location and business needs:
    - Leased Lines (Ethernet Services): Dedicated, high-speed, synchronous connections with guaranteed Service Level Agreements (SLAs), ideal for business-critical operations.
    - FTTP Broadband: utilises full fibre optic technology for ultra-fast gigabit-capable speeds, which is less prone to faults than older copper-based services.
    - Standard Broadband/DSL: Provided where fibre is not yet available, though FTTP coverage is rapidly expanding across the UK.
  - **Key Benefits:**
    - Managed Service: Astaris handles everything from procurement and deployment to 24/7 fault monitoring and ongoing support.
    - Resilience: Provides resilient connection options to ensure consistent access to cloud services, crucial as older analogue lines are being switched off.
    - Simplified Management: A single management interface for all IT and communication services and simplified billing
- 

## 3. ROLES & RESPONSIBILITIES

- Proactive monitoring and maintenance of all specified IT assets.
  - Ensuring systems are secure, up-to-date, and reliable.
  - Adherence to agreed Service Level Agreements (SLAs).
  - Providing clear reporting on system health and service performance.
  - Managing the transition process from the incumbent
-

## 4. SERVICE LEVELS & PERFORMANCE MONITORING (SLA)

Astaris utilises automated remediation scripts for common issues to ensure rapid resolution.

Astaris commits to meeting the Incident Response Times as set out below:

| <b>PRIORITY CODE</b>              | <b>URGENCY (Status of service)</b>                                                                                                  | <b>INCIDENT RESPONSE TIMES</b>                                                                         | <b>UPDATE FREQUENCY</b>            | <b>RESOLUTION AIM</b>                             |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------|
| ACTIVE CYBER ATTACK<br>Priority 0 | Most urgent possible response if an active ransomware attack is ongoing                                                             | Instant if raised by phone                                                                             | Open phone line / constant updates | ASAP                                              |
| CRITICAL<br>Priority 1            | For all users:<br>-Service totally unavailable<br>-Interferes with normal completion of work<br>-no work around                     | Critically important - respond < 10 mins if raised by email. Respond instantly if raised by phone call | 15 mins                            | 2 hours remote<br>2 hours + travel time if onsite |
| HIGH<br>Priority 2                | Service failure affecting group of users                                                                                            | High Importance - respond < 30 mins                                                                    | Every hour                         | 4 hours remote<br>4 hours + travel time if onsite |
| NORMAL<br>Priority 3              | - Tasks are made more difficult but not impossible to complete - has workaround<br>- Performance poor or unacceptably slow          | Normal - respond < 4 hours                                                                             | Twice daily                        | 1 working day remote<br>2 working days if onsite  |
| LOW<br>Priority 4                 | Issue affecting 1 user that has workaround                                                                                          | Respond < 1 working day                                                                                | Every working day                  | Best Effort/ 3 days                               |
| LOW<br>Priority 5                 | Interferes with recreational or non-business related use. Service request - non service affecting task - i.e., new starters/leavers | Respond < 2 working days                                                                               | 5 working days                     | Best Effort/ 5 days                               |

## 4.1 KEY PERFORMANCE INDICATORS (KPIs) & MONITORING

KPI's may apply to areas such as first contact resolution, response times, ticket escalation etc. Performance is monitored using the Astaris ticketing portal. Your appointed representative will have real-time access to the portal to track ticket progress, SLA compliance, and generate reports. Detailed reports of system health, status, and resolved issues will be generated monthly and automatically distributed to the Office Manager (or the person client has designated as the primary point of contact).

---

## 5. SUPPORT & INCIDENT MANAGEMENT

### 5.1 HOW TO ACCESS HELP & REPORT ISSUES

Users can access support and report any issues via multiple channels, all seamlessly integrated into the Astaris ticketing system. An email notification is automatically generated for the user whenever a ticket is updated, keeping them informed of the Status.

- Email: Send an email to [support@astaris.co.uk](mailto:support@astaris.co.uk). A ticket and automatic acknowledgment are generated instantly. (24x7 availability)
- Telephone: Call the main Astaris number. A support agent will raise a ticket during business hours.
- Ticketing Portal: Direct access to the online portal for raising tickets. (24x7 availability)
- Laptop Widget: Use the direct access widget on the laptop to raise tickets easily, with the option to include screenshots. (24x7 availability)
- Online Chat: Via the Astaris website during business hours.

The customer's office representative has access to the ticketing portal to view the status of all tickets, monitor performance, and generate reports on time taken and SLA compliance. All tickets include a "rate our response" section for user feedback

### 5.2 HOURS OF OPERATION

Standard Support Hours: Monday to Friday, 08:30 to 17:30.

Out-of-Hours Emergencies: Available 24x7x365 by calling the main Astaris telephone number, which forwards calls to the on-duty engineer. There is no extra charge for emergency calls.

### 5.3 SUPPORT SCOPE & LIMITATIONS

- Unlimited Support: Telephone, email, and remote support are unlimited in quantity and cover all "business as usual" maintenance and requests.
- Out-of-Scope Work: New functionality or stand-alone projects fall outside the scope of standard support but can be quoted as fixed-price projects.
- Out-of-Hours Limits: There are no limits on the amount or type of emergency support offered when called via the emergency number.
- Escalation and Workarounds: Timescales may be extended due to complexity or third-party dependency. Astaris will use reasonable endeavors to eliminate or reduce impact by providing a workaround.

### 5.4 SCHEDULED & EMERGENCY MAINTENANCE

- Astaris may interrupt the Service for Maintenance Events. Astaris shall use reasonable endeavors to ensure that:
  - Scheduled Maintenance will not exceed 3 hours in any calendar month.
  - Emergency Maintenance will not exceed 3 hours in any calendar month.
- Astaris will provide a minimum of 1 Business Day advance notice for Scheduled Maintenance Events where possible.
- Maintenance Events that occur during Normal Business Hours, and which were not requested by the Client, shall be considered downtime for service availability measurement purposes.

### 5.5 ON-SITE SUPPORT

While support is primarily delivered remotely to ensure the fastest possible response times, we are committed to providing on-site support whenever a technical challenge cannot be resolved through remote intervention.

- Emergency Call-Outs: Astaris internally treats the need for an emergency onsite call-out as a serious service failure, with an expectation of less than one per year post-onboarding.
- Onsite Service: If the Client requests onsite service and no problem is found or reproduced, the Client shall be billed at the applicable rates.
- Additional planned visits at the request of the Client.

All pricing for on-site and remote support services is provided in the Pricing Document and is based on the published rate card.

### 5.6 ISSUE RESOLUTION

All recorded issues follow a defined process:

1. Initial triage, issue replication, and diagnosis.
2. Assignment to an Astaris support technician.
3. Tracking progress within the portal, visible to the customer's Office Manager (or person the client has designated as the primary point of contact).
4. If an issue is not resolvable by Astaris, or is a vendor issue, Astaris will escalate to the third party and retain ownership until resolved.

## 5.7 COMPLAINTS HANDLING & ESCALATION

Should any user be dissatisfied with any aspect of the service, the first escalation should be to our Service Desk Manager, followed by escalation to Head of Technology. There are detailed internal processes for dealing with complaints that follow ITSM, ITIL and ISO9001 paths. Complaints are always seen as an opportunity to solicit honest feedback and use it to improve our systems / processes.

## 5.8 DATA SECURITY MANAGEMENT

Security is central to Astaris' operations, ensuring robust data security:

- **Backup Solution:** A Tier 1, SOC2 certified, GDPR compliant backup solution secures all Office 365 data with a 15-minute Recovery Point Objective (RPO) and a less than one hour Recovery Time Objective (RTO).
  - **Security Measures:** The overall security posture is maintained through measures including Bitlocker, password management tools, mandatory 2FA on all systems, formal onboarding/offboarding processes, least access principles, BYOD/conditional access policies, provably restorable backups, network segmentation, vulnerability/patch management, on-device protection, user awareness training/phish testing, and content filtering.
- 

# 6. SECURITY & STANDARDS

## 6.1 CERTIFICATION & STANDARDS

Astaris operates within accredited frameworks to ensure high quality and secure service delivery:

- ISO 9001 (Quality Management)
- ISO 27001 (Information Security Management)
- Cyber Essentials

## 6.2 DATA SECURITY MANAGEMENT

- **Tool Access:** Astaris support technician access to management tools is tightly controlled, protected with Two-Factor Authentication (2FA), and subject to in-depth logging and auditing of all actions performed.
  - **Data Location:** Data is stored within EU and UK datacenters where possible for GDPR compliance.
  - **Hardware Disposal:** Data removal and destruction on disposed hardware is performed securely. Devices are either reused for charity (after data sanitization) or sent for fully WEEE-compliant disposal via an accredited third party.
-

## 7. SERVICE MANAGEMENT

### 7.1 ONBOARDING PROCESS

Astaris provides a structured five-stage onboarding and transition process designed to migrate organisations from legacy systems to modern cloud environments with zero downtime. We prioritise a heavy initial investment in documentation and infrastructure takeover to ensure your systems are reliable, secure, and remotely manageable from day one.

### THE ASTARIS ONBOARDING & TRANSITION PROCESS

**1. Discovery & Documentation:** The process begins with a formal handover from your incumbent provider. Astaris engineers conduct a comprehensive onsite survey and deep-dive audit of your IT estate—including user profiles, licenses, and network architecture—to create a custom "Onboarding Roadmap."

**2. Strategy & Technical Design:** We finalise your cloud architecture (e.g., Microsoft 365 or Google Workspace) and configure a secure identity posture using Microsoft Entra and Cisco Umbrella. During this phase, any legacy technical issues are "ironed out" to ensure you start our service with a clean, optimised environment.

**3. Phased Infrastructure Takeover:** The physical transition moves into an active phase, starting with the takeover of network infrastructure (firewalls, Wi-Fi), followed by cloud services, and concluding with the enrollment of all computer and server infrastructure into our management tools.

**4. Implementation & Security Hardening:** Astaris handles the secure migration of emails, files, and databases while applying mandatory G-Cloud 15 controls. This includes Cyber Essentials compliance, Multi-Factor Authentication (MFA), and enrolling mobile fleets into Microsoft Intune for strict policy enforcement.

**5. User Training & Handover:** To ensure immediate productivity, we offer flexible training delivered by qualified engineers—available either onsite or via remote 1-1 and group sessions. Every user receives a "How to Get Started" guide and clear instructions for accessing our 24/7 technical support.

Once complete, all bespoke configurations and site data are logged in our centralised knowledge base. This allows our support departments to provide informed, proactive assistance as your organisation transitions into our "Always-On" managed service.

## 7.2 OFFBOARDING PROCESS

### THE ASTARIS OFFBOARDING PROCESS

Our offboarding process ensures that when a client exits the framework or transitions to another provider, their data remains protected, accessible, and fully owned by them, with zero service disruption.

**1. Strategy & Exit Planning:** We work with the client to define an exit strategy. This includes identifying all data locations, service dependencies, and the final "termination" date to ensure a smooth transition without data loss.

**2. Data Extraction & Portability:** Astaris provides all customer-owned data in a structured, industry-standard format (such as .PST for email or .CSV/.ZIP for files). We ensure that all data is portable and ready for migration to a new provider or an on-premises system.

**3. Access & Identity Revocation:** Once the migration is confirmed, we systematically revoke administrative access. This includes decommissioning relevant Microsoft Entra (Azure AD) identities, removing devices from Microsoft Intune, and disabling security agents like SentinelOne and Cisco Umbrella.

**4. Security & Compliance Sanitization:** To meet GDPR and Cyber Essentials standards, Astaris performs a secure "data wipe" of any cached information on our internal management systems. We provide a formal confirmation that all client data has been deleted from our infrastructure while the client retains the master copies.

**5. Handover & Final Documentation:** We provide a final documentation pack to the new provider or the client's internal team. This includes network diagrams, license schedules, and an inventory of assets to ensure the new team has everything they need to maintain the environment.

### 7.3 Rates for Out-of-Scope Work

Where the Customer requests professional services outside the defined scope of the support contract, such services will be provided in accordance with the published rate card and only following written agreement on scope, duration and cost prior to commencement.