



TRANSFORMING BUSINESS
THROUGH **TECHNOLOGY**

End User Compute Managed Service

SERVICE OVERVIEW



Contents

1.	Why Core?	3
2.	Core Managed Services – Overview	4
3.	End User Compute Managed Service Overview	5
4.	End User Compute	6
4.1.	Physical Windows Desktop Support Detail	6
4.2.	MacOS Support	7
4.3.	Windows 365 Support Detail	7
4.4.	Mobile Support Detail (MDM)	8
4.5.	Application Packaging	8
5.	Service Level Agreement	9
5.1.	Incidents	9
5.2.	Service Requests	10
6.	Prerequisites, Environments, Inclusions and Exclusions	12
6.1.	Prerequisites	12
6.2.	Inclusions	13
6.3.	Exclusions	13
6.4.	Definitions	14
7.	Commercial	15
7.1.	Customer Responsibilities	15
8.	About Core	16

Please note that information contained within this document is classified Commercial in Confidence and should not be shared with any third parties without the express written permission of Core Technology Systems (UK) Ltd.



1. Why Core?

Your organisation deserves reliable, trustworthy, and responsive expert IT support so you can focus on what you do best. With our 32-year history, your business is in capable and experienced hands. In 2001, Core deployed the first installation of SharePoint in the UK and have continued to deliver and support Microsoft products and solutions, leading businesses to superior levels of productivity, security, and growth. From the early operating systems and intranet solutions to the advanced productivity and security tools that organisations adopt to seek efficiencies, Microsoft solutions now touch tens of millions of lives daily; and Core helps to optimise solutions for your desired outcomes.

Core is a Microsoft Modern Workplace Advanced Partner and has been delivering Microsoft solutions for nearly three decades; transforming, enabling, and securing our customers with the evolution of Microsoft business technologies across the UK.

Our focused expertise and experience, along with our long-standing relationship with Microsoft, means that when our customers invest in world-class transformation products, they are delivered by our team of leading experts, and managed personally, with competence.



Infrastructure
Azure
Digital & App Innovation
Azure
Data & AI
Azure
Security
Modern Work



Simplicity

Our Managed Services have been designed to serve your business needs, whatever your internal IT support capabilities. Additionally, with more than three decades of developing relationships with IT decision makers, the simplicity of our Managed Service offerings reduces the complexities of support; allowing you to make the best decisions for your organisation and providing a clear delineation of internal and external roles.



Transparency

This transparent and modular Managed Service packaging enables you to choose between fully outsourcing your IT Management, or strategically outsourcing select components.



Flexibility

Experience has taught us that some customers may wish to customise these options, tailored to their specific requirements, and we want you to feel confident in the decision to partner with Core. If you would like a tailored solution, please talk to your account manager who will be happy to discuss your requirements.



Optimisation

Subscription to Core's Managed Services offers the potential to unlock flexibility, resilience, and enhanced team performance, striking the perfect balance between in-house responsibilities, and Core's Managed Services. Whatever your internal capabilities, and whatever your infrastructure, Core can provide the enterprise-level support your business needs.





2. Core Managed Services – Overview

Our range of Managed Services are modular, allowing you to select exactly what you need, when you need it, knowing that with more than three decades of Microsoft heritage, *Core can deliver.*



Managed Services

- Infrastructure as a Service
- End User Compute
- Service Desk
- Teams Calling
- IT Security
- Network Infrastructure
- Windows Server



Support Services

- Microsoft 365 Support
- Dynamics CRM Online Support



Solutions

- Core Membership Management
- Core Identity and Access Management
- Core Intranet and Digital Workspace Management
- Core Document Management



Smart Services

- Smart Projects
- Smart Resourcing



Professional Services

- Core Project Management
- Core Enablement



Quick Deploy

- Viva Connections Quick Deploy
- Viva Suite Quick Deploy



3. End User Compute Managed Service Overview

Core's EUC Managed Service offering has been designed from more than three decades of experience delivering Microsoft solutions.

Employee requirements are changing, the needs of businesses are changing, but more importantly, the technology to meet these requirements is already here.

Our EUC Managed Service supports physical desktop, Windows 365, Mobile and MacOS environments, making it the go-to service for organisations looking to simplify workflows, maximise productivity, and improve efficiencies. See [Section 5](#) for details about how your business can benefit from our EUC Managed Service.



2nd & 3rd Line Service Desk for EUC Managed Service issues

Provides escalation point for internal or external IT functions.



Platform Change Management

Device and Application management policy updates & assignment.



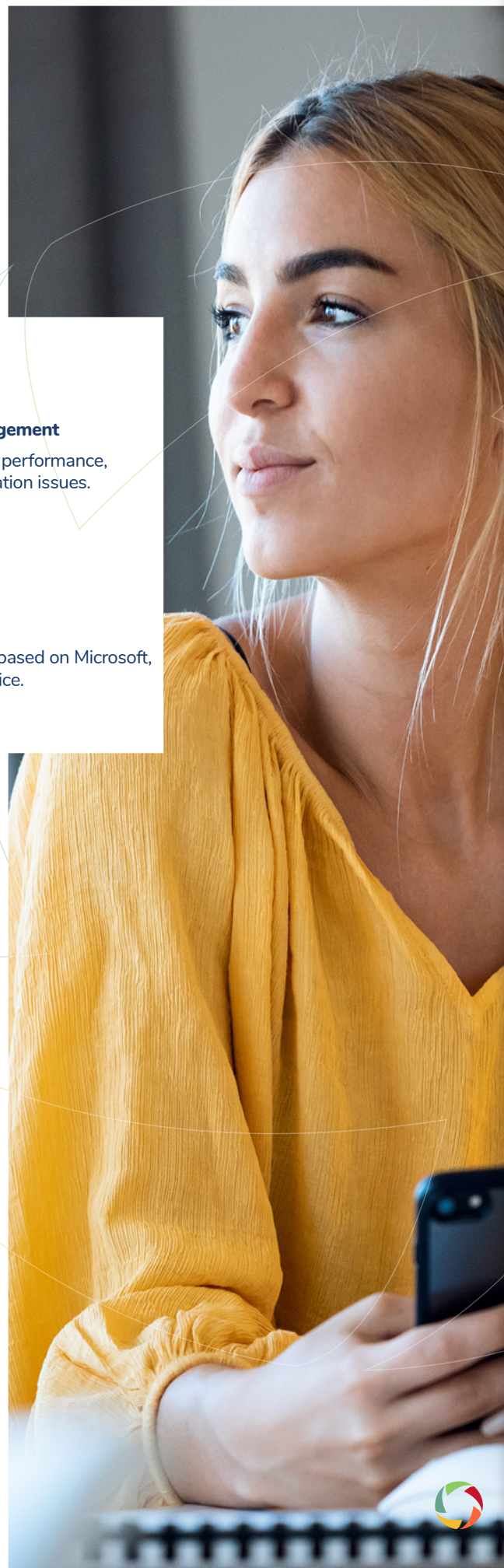
Platform Incident Management

Remediate EUC platform performance, compliance and configuration issues.



Platform Security

Default platform policies based on Microsoft, CIS and NCSC best practice.



4. End User Compute

4.1. Physical Windows Desktop Support Detail

The following table details the support available for your Physical Desktop Windows 10/11 environment:

Feature	Description
Incident Management	Manage escalations of incidents related to device provisioning , application deployment, configuration or performance that cannot be resolved by first line teams.
Hardware Provisioning	Provisioning of new corporate Windows 10 & Windows 11 devices via Microsoft Intune (Autopilot), following the registration of device hashes into Intune.
Device Configuration	Manage requests that involve modifying the configuration profiles & policies applying to devices to either enable or disable specific features.
Device Security	Manage requests that involve changing the security posture of devices through security policy management, including attack surface reduction rules, Microsoft Defender, firewall policies, USB access policies.
Intune Environment	Manage the Microsoft Intune environment configurations that are relevant to Windows devices.
Browser Management	Manage browser security through policy and the approval of browser extensions.
Hardware & Boot Up Remediation	Investigate and resolve issues relating to failed boot, hardware, and hardware OS malfunctions. Reset the device and/or arrange for replacement as appropriate.
Lost & Stolen	Should a hardware device be reported lost or stolen, our Service Desk will implement device wipe procedures where supported by the service.
Hardware Retirement	Upon completion of an agreed service period, hardware will be decommissioned in accordance with client policies. All data will be wiped, and the device will be removed from Intune.
Application	Configuration and deployment of applications available through automated package management services where supported. Manual packaging services are available for a fee.
Azure Active Directory	Administrate aspects of Azure AD required to manage the EUC service, such as group creation / membership management, and device management.
Device Upgrades	Manage Windows feature update releases in line with Microsoft release cycles with at least one feature update completed per year.
Group Management	Resolve issues with user and device group profiling and policy enforcement.
OS Patching (Quality Updates)	Operation system and application monthly patching via Microsoft Intune for the Operating System. For Zero-Day vulnerabilities, manage emergency patching procedures to ensure timely updates to devices.
Application Patching	Management of patching of applications supported by deployed automated package management services.
Reporting	Self-service reporting will be made available in a log analytics workspace. Core will provide a workbook with a variety of self-service reports for the environment.



4.2. MacOS Support

Feature ¹	Description
Device Provisioning	Self service Enrollment or automatic enrolment into Microsoft Intune for a new macOS device. After entering credentials, the device registration completes, installs Company Portal and prompts for corporate login. Provide assistance to users with the enrollment process. Perform device resets as required.
OS Management	Enforcement of device configuration, and compliance policies for the local device using Microsoft Intune features.
Lost & Stolen	Devices are logged as being lost or stolen, devices are removed from Microsoft Intune, user accounts reset, and MFA sessions cancelled. A remote wipe is triggered on the device. Device release within Apple Business Manager.
Hardware Retirement	Upon completion of an agreed service period, hardware will be decommissioned in accordance with. All devices will be removed from Intune and device release within Apple Business Manager.
User Profiles	Remediation of issues relating to individual user profiles.
Apple Business Manager	Management of the Apple Business Manager or Apple School Manager account including associated devices, applications and tokens.
Security	Management of device security configuration, and malware protection using Microsoft Defender for Endpoint. Configure disk encryption on the device.
Apple peripheral support	Troubleshoot and assist users with USB and Thunderbolt peripherals connected to macOS devices.
Applications	Remediation of issues relating to application assignment and deployment, management of applications through the Apple App Store, and deployment of custom line of business applications.
Azure Active Directory	Administer Azure AD groups and users in relation to the management of the macOS support service and application assignments.

¹ Features available in support may vary based on the macOS enrollment method.

4.3. Windows 365 Support Detail

The following section details the support capabilities available for your Windows 365 Environment:

Feature	Description
CloudPC Provisioning	Manage user license assignment and provisioning policy management. Manage requests to change provisioning policies, and ensuring image versions are supported versions. Where required reprovision Cloud PC's to remediate issues.
Application Packaging & Deployment	Where enrolled in Microsoft Intune, deploy application that can be managed through automated package managers. Assign existing applications to CloudPC's or users.
Device Compliance Management	Ensure Cloud PC's maintain compliance in Intune and adhere to conditional access policies. Service requests to place Cloud PC under review. Centrally manage application deployment.
User Profile Management	Incident and Service Request processing for problems relating to profile containers including cache performance, OneDrive Sync, additional user folders.
Device Data Management	Where supported manage requests to create Cloud PC restore points, or perform Windows 365 point in time restores.
Active Directory Single Sign On	Administrate Azure AD to remediate incidents related to the management of the mobile support service.
Patching	Cloud PC Monthly patching in line with Microsoft Release cycles. Reprovisioning of Cloud PC's where required to maintain supported version compliance. Expediated patching for Zero-Day vulnerabilities.



4.4. Mobile Support Detail (MDM)

The following table details the support available for your Mobile device (MDM) environment:

Feature	Description
Device Provisioning	New corporate mobile device provisioning via Microsoft Intune.
Device Issues	Investigate device related issues relating to operating system malfunction, device profiles & policies or OS updates.. Arrange for replacement devices as appropriate.
Lost & Stolen	Should a hardware device be reported lost or stolen, device wipe procedures where supported to remove corporate data.
Hardware Retirement	Upon completion of an agreed service period, hardware will be decommissioned in accordance with client requirements. All data will be wiped, and the device will be removed from Microsoft Intune.
Device Configuration	Manage set of secure policies based on prevailing best practices for Corporate and BYOD mobile devices. Ensuring Corporate and personal data separation on BYOD Devices (MAM). Manage requests to change configuration or security policies being applied to devices. Periodically review policy sets against prevailing best practices from Microsoft, CIS and NCSC.
Account and Application	Management of application publication from Apple Store or Google Play Store. Management of Apple Business/School manager and Android Enterprise business accounts and Microsoft Intune Integration.
Azure Active Directory	Administer Azure AD groups and users in relation to the management of the mobile device support service and application assignments.

4.5. Application Packaging

The application packaging service will take a vendor provided application installer and prepare it for deployment within Microsoft Intune.

Feature	Description
Standard Application Packaging	Package application as a one-off service on a first in first out basis (except for premium packaging). Applications are prepared for deployment and depending on the complexity, an associated script or installer modification is configured. Application package is uploaded to Microsoft Intune and is made available to users or devices based on the request details.
Priority Application Packaging	Package application as a one-off service on a first in first out basis. Any priority requests are processed before standard requests in the queue. Applications are prepared for deployment and depending on the complexity, an associated script or installer modification is configured. Application package is uploaded to Microsoft Intune and is made available to users or devices based on the request details.
Evergreen Proactive Subscription ¹	Core will track a named list of application versions, regularly checking with the vendor website for updates. Where an update is identified, it will be packaged and staged for deployment ² .

¹ Subscription services have a minimum quantity of 5 applications and are for a minimum term of 12 months.

² Customer will need to provide Core login access to vendor portals where installers are only available post login.



5. Service Level Agreement

- Our Service Desk can be reached by raising a ticket through <https://service.core.co.uk>. Alternative methods of reaching the service desk are calling **+44 207 953 3699** or by emailing servicedesk@core.co.uk to log any incidents or service requests.
- Core will provide a Service Desk ticketing solution to enable internal IT Service Desk Analysts to log and record tickets.
- Core provide a helpdesk available for agreed service hours for working on incident tickets.
- Tickets will be placed on hold while waiting for a response from users.
- Tickets are closed when the user is happy the issue, request has been resolved or there is no response from the user after 3 contact attempts.
- Core Service Desk and the Managed Service team is ISO:27001 compliant. Services are provided in accordance with ITIL Service Management best practice framework.

5.1. Incidents

Below is a breakdown of our SLA definitions, along with response and resolution times:

Priority Level ¹	Definition	Resolution ²	KPI
Priority 1 	Complete loss of business-critical systems. Critical business impact. Complete service failure or inaccessibility of critical functionality. No acceptable workaround available.	4 hours	90%
Priority 2 	Partial loss or degradation of a supported service. Serious business impact. Widespread degradation of a service or failure of functionality of critical system. No acceptable workaround available.	8 hours	90%
Priority 3 	Low Impact: business-critical systems unaffected, more than one user affected. Partial/intermittent application degradation or loss of functionality. Typically impacting a subset of users. No direct impact on services availability. A workaround is available.	3 business days	90%
Priority 4 	Minimal impact to non-critical systems. Single user affected. Application or personal procedure unusable. A workaround is available, or a remediation is possible.	4 business days	90%

Notes:

¹ Core may downgrade the severity level if the customer is not able to provide adequate resources or responses to enable Core to provide continuous problem resolution efforts.

² Standard incident support hours are from 09:00 - 17:30 GMT/BST Monday to Friday excluding UK public holidays.



5.2. Service Requests

Priority Level ¹	Definition	Resolution ²	KPI
Priority 1 	Emergency Request. Emergency Request. Emergency service requests require completion within accelerated timescales, to avoid an interruption or unacceptable risk to the customer's business. An example would be a user account requiring locking due to an immediate dismissal; a backup recovery being required to enable staff to work. ³	4 hours	90%
Priority 2 	Expedited Request. Expedited service requests are service catalogue items that require expediated delivery. Examples include emergency software patch updates.	8 hours	90%
Priority 3 	Standard Request. Standard requests are pre-defined within the service catalogue and can be delivered as standard (pre-approved) changes.	3 business days	90%
Priority 4 	Low Priority Request.⁴ Examples include information requests and requests that may require submission for change approval.	4 business days	90%

Notes:

¹ Core may downgrade the severity level if the customer is not able to provide adequate resources or responses to enable Core to provide continuous problem resolution efforts.

² Standard service request hours are from 09:00 - 17:30 GMT/BST Monday to Friday excluding UK public holidays.

³ Subject to fair use policy.

⁴ Requests requiring full change will be placed on hold pending the change approval process.



6.3 Application Packaging

Priority Level	Description	SLA ¹	KPI
Priority 	Priority application packaging service for applications that need to be packaged and made available to devices on accelerated timescales.	24 Hours (3 Working Days) ²	90%
Standard 	Application packaging service to package and make applications available to devices.	40 Hours (5 Working Days) ²	90%

Notes:

¹ Standard service request hours are from 09:00 - 17:30 GMT/BST Monday to Friday excluding UK public holidays.

² All packaging requests go through a thorough triage process. For any applications that are assessed to have complex packaging they will be excluded from SLA, and the customer informed of expected timescales.

6.4 KPI's

Described below are the key performance indicators for the Microsoft Windows DaaS Service.

DaaS Function	Description	Measure	KPI ²
Windows Device Patching	% of available devices up to date with latest Microsoft O/S Patches	Patching Coverage	90% of active ¹ devices to be up to date with patching.
Windows Patch deployment timeliness⁵	Measure of the speed of deploying Microsoft patch Tuesday monthly updates.	Speed of patch deployment	90% of active ¹ devices within 14 days.
Windows Emergency Patches	Measure of the speed of deploying emergency patches available from Microsoft.	Speed of emergency patch deployment	90% of active ¹ devices within 2 working days.
Windows Feature Updates	Measure the speed of Microsoft Feature ³ update rollout.	Feature Level Compliance	90% of active ⁴ devices upgraded within 6 months of Feature update availability.

Notes:

¹ Active is defined as the average of the number of devices that have synchronized with Microsoft Intune in the last 14 days preceding the activity start.

² The KPI's apply to devices running Core's standard build and is dependent on using the required reporting platform.

³ Feature updates do not include changes in the Windows major version. E.g., Windows 10 to Windows 11.

⁴ Active is defined as the average number of devices that have synchronized with Microsoft Intune in the last 14 days preceding the activity end.

⁵ This KPI does not apply to the standard SKU.



6. Prerequisites, Environments, Inclusions and Exclusions

Please take the time to review and understand the below Prerequisites, Inclusions and Exclusions. We understand that customer environments are all unique and can accommodate variations, as necessary. Should you have any concerns regarding your environment, please raise this with your account manager.

6.1. Prerequisites

- Customers are required to have in place suitable license subscriptions prior to subscribing to Core's Managed Services. Managed service capabilities are dependency on available licensed features. Our helpdesk cannot undertake incidents on unlicensed software, or aid in the procurement of licenses.
- Conditional Access Policies and Remote Tools must be preconfigured as part of an onboarding Professional Service engagement to take advantage of Core's Managed Service offerings.
- Acceptance of a Microsoft Granular Delegated Access Permission (GDAP) request to allow the managed services teams access to the environment. Auditing is provided on the client side.
- Acceptance of an Azure Lighthouse request so that the self-service reporting environment can be maintained.
- Azure Subscription with an Azure Monitor Log Analytics workspace to support self-service reporting.

6.1.1. Windows 10 and Windows 11 Support

- Windows 10 & 11 Professional and Enterprise editions, and the educational equivalents.
- Professional edition must be installed from professional media, with a suitable license key.
- Single user, and multi-user device configurations available.

6.1.2. MacOS Support

- For Automatic device enrollment support, the service requires the device to be added to Apple Business Manager, or Apple School Manager ideally at the time of purchase by an authorised reseller.
- Enrolling a device with Automatic Device Enrollment requires the device to be reset.
- For self-service enrollment, the user is required to download and install Microsoft Company Portal, and sign-in with their Azure AD credentials.
- Devices can be enrolled into Apple Business Manager, or Apple School manager retrospectively with the following restrictions:
 - Mac computer is running with Apple Silicon or with an Apple T2 security chip
 - Mac computer needs to be running macOS 12.0.1 or later
 - The registration process requires Apple Configurator running on an iPhone with iOS 15 or later, and the iPhone will need to be local to the Mac
 - Currently configured in-use devices will need to be reset
 - Devices are associated with a single user
- User will be required to sign-in to the Microsoft Company Portal application where applications will be made available. For both deployment options.
- The service does not support SSO authentication with Azure AD
- Application deployment supports PKG and DMG files



6.1.3. Windows 365

The Windows 365 service has the following pre-requisites:

- Windows 365 Business and Enterprise licenses can be supported.
- Intune is recommended with Windows 365 Business, and requires manual enrollment.
- Cloud PC's are assigned to a single user, but a user can be assigned multiple Cloud PC's of different sizes.
- For service billing Windows 365 Frontline counts the number of provisioned Cloud PC's.

6.1.4. General Licensing

- Microsoft 365 Enterprise (Business premium/E3/E5) Licenses recommended.
- Service can also support Individual SKUs consisting of
- Intune or Enterprise Mobility Suite
- Azure AD P1/P2
- Windows 10/11 Enterprise (E3/E5)

6.2. Inclusions

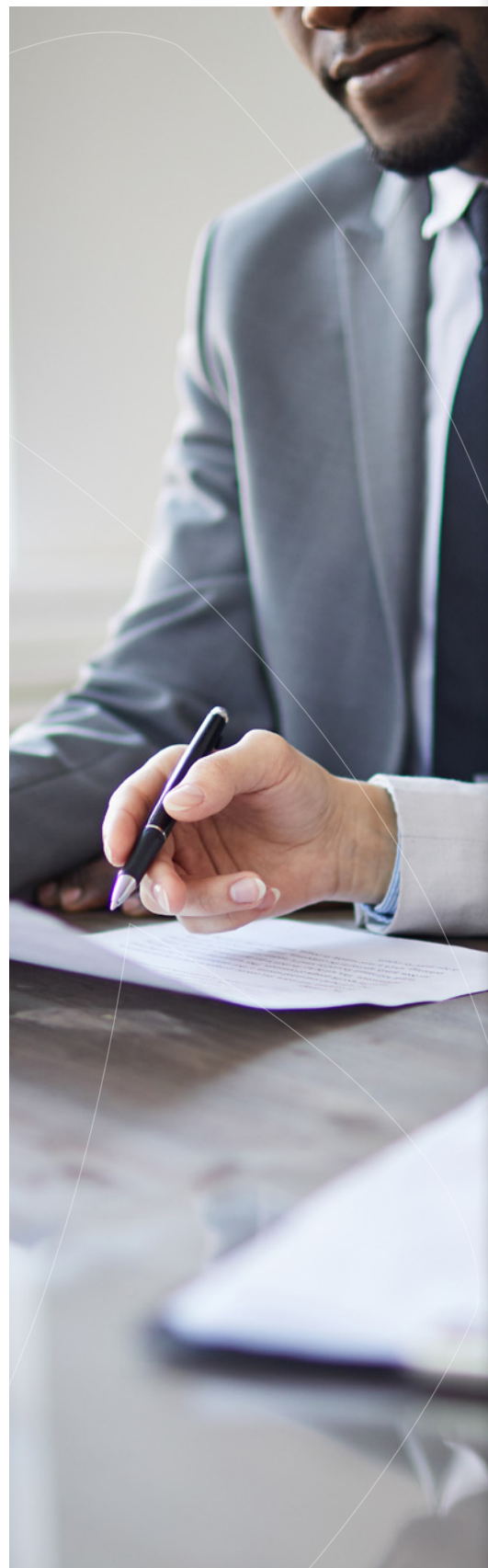
The service outlined in this document provides operational support for the following Microsoft devices and platforms only:

- Windows 10, and 11 Managed Device
- Windows 10, Windows 11 Professional and Enterprise, and Education equivalents.
- Windows 365 Business and Enterprise
- macOS operating system
- Mobile Devices (iOS, iPadOS and Android)
- Azure Active Directory (Service specific)
- Available service requests are dependent on the service tier selected.

6.3. Exclusions

The items below are not included as part of Core's Managed Service Desk but may be added via additional Managed Services. Please enquire for any costs not shown in this information pack:

- All software licensing
- All hardware including desktops, laptops, tablets, and mobile phones
- Windows 10/11 Home Editions, or Home Editions upgraded to Professional through the Microsoft Store.
- Maintaining application patching to Cyber Essentials standards.
- Dedicated Service Manager



- Automation or integration of 1st Line support into Core service desk (where 1st line support is not being delivered by Core)
- Application licensing
- Application support, covering specific application usage scenarios, or user specific configurations.
- Application migration
- Application virtualization
- Dedicated Customer Success Manager.
- Disaster Recovery Services
- Business Continuity Services
- Professional services relating to onboarding activities
- Professional services relating to offboarding activities
- On-site support
- Training
- eDiscovery or investigations within the Office 365 platform
- Conditional Access Policies and Devices - must be preconfigured by the customer or as part of an onboarding Professional Service engagement to take advantage of the Core EUC Managed Service
- Azure Active Directory - whilst AAD plays a significant role in underpinning all Azure services, Core's support in this instance is restricted to features that facilitate the operations of our Managed Services. More advanced support for a broader range of Active Directory services for security, governance and compliance capabilities are available via additional Managed Services

6.4. Definitions

Please refer to the below definitions of terminology used throughout this document and our other Managed Service Descriptions:

Customer

The company receiving the purchased service.

End-user

Customer employee included in the Managed Service Desk agreement.

End-user device

Customer hardware, such as a laptop or desktop, used by end-users included in the Managed Service Desk agreement.

Escalation

Depending on the severity or technical requirements of an incident or request, a Service Desk analyst may pass the ticket to a 2nd line or dedicated team. Escalation paths are agreed during the customer onboarding process.

First-time fix

A successful attempt by the Managed Service Provider to resolve a ticket without escalation.

MAM

Mobile Application Management.

Managed Service Provider

The company providing the service – Core Technology Systems.

MDM

Mobile Device Management.

SLA

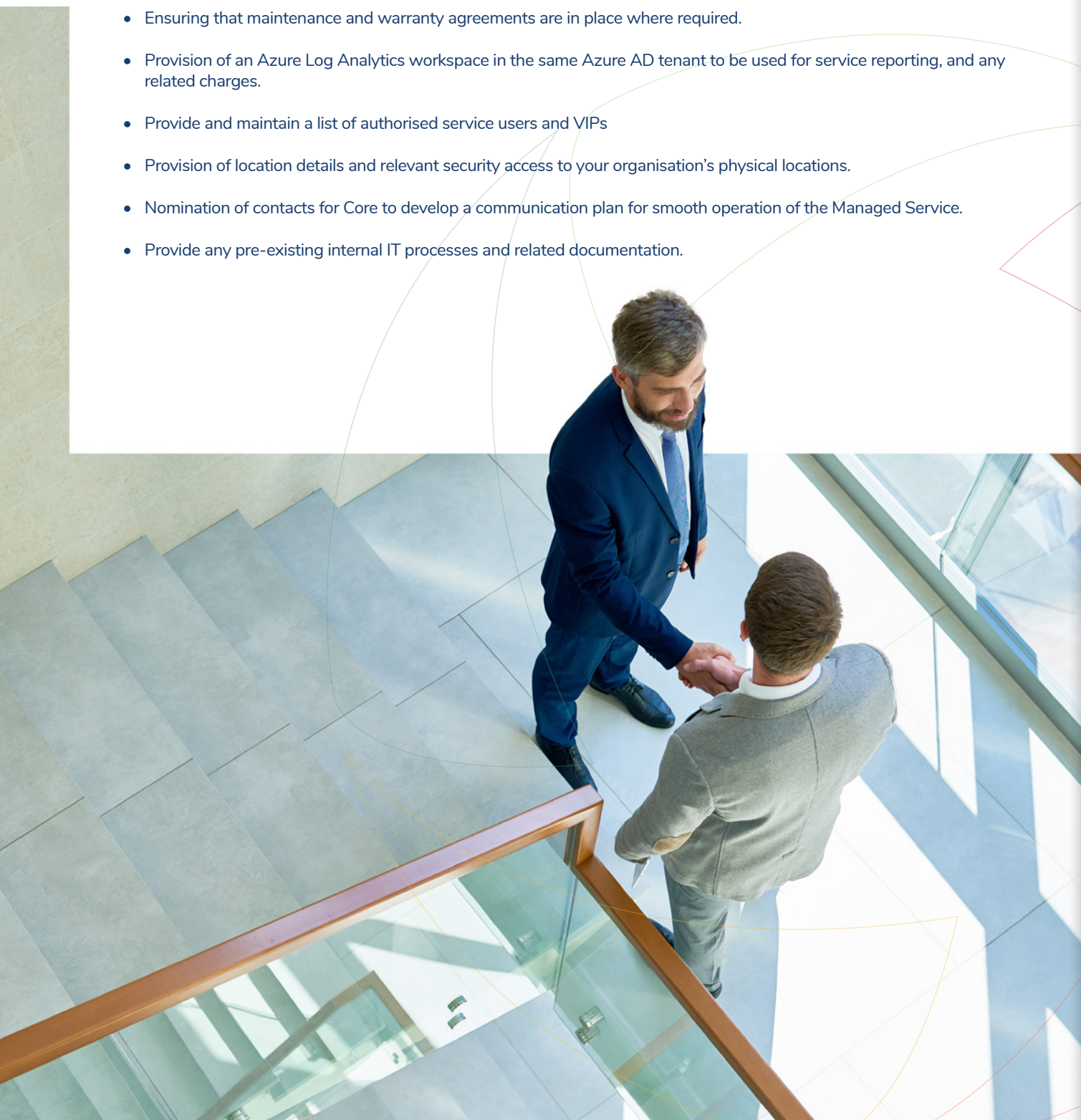
Service Level Agreement. The agreed periods for which a response, and a resolution is expected from the Managed Service Provider.



7. Commercial

7.1. Customer Responsibilities

- As our customer, we will ask you to please provide all necessary information detailing topology, environments, platforms, and systems as part of the process.
- Provision of sufficient access to platforms and systems for Core to deliver the Managed Service.
- Ensuring that the managed environment is sufficiently licensed.
- Ensuring that maintenance and warranty agreements are in place where required.
- Provision of an Azure Log Analytics workspace in the same Azure AD tenant to be used for service reporting, and any related charges.
- Provide and maintain a list of authorised service users and VIPs
- Provision of location details and relevant security access to your organisation's physical locations.
- Nomination of contacts for Core to develop a communication plan for smooth operation of the Managed Service.
- Provide any pre-existing internal IT processes and related documentation.



8. About Core

Core's solutions and services portfolio has been developed from decades of experience. We work closely with Microsoft to ensure that our staff are fully trained and qualified, and the services we provide not only complement the products businesses need today but also incorporate the future plans of our customers.

Microsoft chooses Core as a partner because many of our company values align, and we deliver a great service. The Core values include:



Customers

We put our customers first, taking responsibility for our actions.



One Core

We recruit, develop, and retain the best talent in a supportive environment to best serve our customers.



Responsiveness

We are flexible, approachable, and responsive to our customers' needs.



Expertise

We are professional and constantly strive to achieve excellence for our customers, peers, and partners.

Core has evolved alongside Microsoft's unique offerings to become a leading Managed Service Provider for customers across the UK. Our offering spans the Microsoft suite, from cloud platforms to security and productivity tools. Core has not only been delivering excellent service for Microsoft solutions during the last 30 years of partnership but has also retained specialist talent in our business for decades, that cannot be paralleled by our competitors. We care about our customers and look forward to the opportunity to transform and grow more organisations into the future.



Microsoft
Solutions Partner

What our customers are saying about us



Over the years, Core and the University of Law have built a strong relationship based on trust, expertise and knowledge. We very much look forward to collaborating on future projects with Core.

Tom Brady
University of Law

[Read case study](#)



Viva Connections was a really good find – a starting point that puts us in a good place for future projects, plugged into a really strong, easy-to-use infrastructure.

David Thackray
Hythe Group

[Read case study](#)

