1. Service Overview

Our Modern Device Management Service offers centralised control of your end-user devices including Windows 10/11, Android, iOS, macOS.

The level of management we provide varies between operating systems and device ownership status based on the supported features for each scenario within Intune and Defender for Endpoint.

For managed Windows 10 and Windows 11 devices, this Service offers provisioning, assigning existing applications from your Intune library, operating system patching, security policies and secure remote wipe at the end of their life.

For managed iOS and Android mobile devices such as those owned by you and issued to your end users for the purpose of their work, this Service offers compliance, application and configuration policies and secure remote wipe at the end of their life.

For unmanaged mobile devices running iOS and Android, such as personally owned bring your own devices, this Service offers mobile application management policies which will only be enforced on supported mobile applications installed on the device when signed into your business context. For a complete list of supported mobile applications please refer to the Microsoft documentation on their website.

For all macOS devices running macOS 10.15 or later, this Service offers policy management and application assignments limited by those natively supported in Intune. Operating system patching is not included for macOS devices.

This Service does not provide any management for servers or Linux end user devices.

2. Service Specific Deliverables

This Service is offered in two (2) tiers, Business and Enterprise. The tier you are eligible for is dependant on the type of Microsoft 365 licences you have in your environment as they determine which Microsoft 365 device management features we can enable for you and how we can configure them. The minimum licence requirement for each tier is defined in section 2.1.

Both Service tiers include the features listed in the table below, however certain component or policies associated Intune Baseline are only available for the Enterprise tier (in accordance with Microsoft licence requirement) as specified Section 2.2 below.

Feature
Minimum Licencing Check
Intune Baseline

Microsoft 365 Mobile App Protection
Managed Microsoft Defender for Endpoint Service
Asset List
Platform Support

2.1 Minimum Licencing Check

Your users must have, as a minimum, the following active licences assigned to them prior to us configuring this Service:

(a) Business tier: Microsoft 365 Business Premium.

(b) Enterprise tier: Microsoft 365 E3.

Prior to the setup of this Service, we will review your Microsoft 365 licencing to confirm if you have the minimum Microsoft licences required for each user. If you require additional licences to be added to your Microsoft 365 tenant to enable this Service, we can provide such licences subject to an additional Fee chargeable on a recurring monthly basis.

2.2 Intune Baseline

As standard, we will deliver the services listed in the table below for all compatible devices:

Service
Configuration profiles
Compliance profile
Windows Operating System updates
Application deployment policies
Device provisioning
Device remote wipe
Configuration profiles

(a) Configuration Profiles

We will implement our standard, secure by design, set of Windows 10/11, Android, iOS and macOS configuration profiles in Microsoft Intune and assign these to your users and devices as appropriate.

The standard configuration profiles we implement align, where available and applicable, your environment to the Microsoft baseline, NCSC baselines and the CIS Microsoft 365 Foundation Benchmark E3 Level 1 recommendations.

Further information about the Microsoft, NCSC and CIS baseline recommendations can be found here:

Platform Guides - NCSC.GOV.UK

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

https://www.cisecurity.org/cybersecurity-best-practices/

For Windows 10/11 devices we will also include policies based on the Service tier you have chosen as detailed in the table below:

Policy	Business	Enterprise
Deploy Microsoft 365 applications	●	●
Set desktop background image	●	●
User data backup to OneDrive for Business	●	●
Internet Explorer Enterprise Cloud site list	●	●
Set lock screen image		●
Windows autopatch		●
Proactive remediations		●
Credential Guard		●

(i) Deploy Microsoft 365 applications

We will deploy the Microsoft 365 applications via a packaged Windows 32 application.

(ii) Set desktop background image

If you have procured the Business tier, we will deploy the desktop background from an Azure storage account via a custom PowerShell script. If you have procured the Enterprise tier, we will deploy the desktop background image stored in Azure Storage via a configuration policy.

(iii) User data backup to OneDrive for Business

The data stored in the locations listed below will be automatically backed up to OneDrive for Business. It remains your responsibility to ensure all data created or accessed on your W365 Cloud PCs is backed up to a network or cloud storage location of your choice:

- Desktop;
- My Music;
- My Documents;
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs;
- %APPDATA%\Microsoft\Windows\Start Menu\Programs;

- %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar;
- %APPDATA%\Microsoft\Signatures;
- %LOCALAPPDATA%\Microsoft\Outlook\RoamCache;
- %USERPROFILE%\Favorites;
- %USERPROFILE%\Links;
- %APPDATA%\Microsoft\Excel\XLStart;
- %APPDATA%\Microsoft\Word\STARTUP;
- %LOCALAPPDATA%\Microsoft\Outlook;
- %APPDATA%\Microsoft\Templates;
- %LOCALAPPDATA%\Microsoft\Office;
- %APPDATA%\Microsoft\Sticky Notes; and
- %LOCALAPPDATA%\Google\Chrome\User Data\Default.

(iv) Internet Explorer Enterprise Cloud site list

This policy configures devices to use an enterprise cloud site list held in the Microsoft 365 admin center. An enterprise site list tells legacy websites to use Internet Explorer mode within Microsoft Edge.

(v) Set lock screen image (Enterprise Tier Only)

We will configure the lock screen image stored in Azure Storage via a settings catalogue policy.

(vi) Windows autopatch (Enterprise Tier Only)

We will configure Windows Autopatch, a cloud service that automates Windows 10 or 11 enterprise operating systems, Microsoft 365 Apps for enterprise, Microsoft Edge, and Microsoft Teams updates.

(vii) Proactive remediations (Enterprise Tier Only)

We will configure the proactive remediation feature included in your Enterprise tier. Proactive remediations are script packages that can detect and fix common support issues on a user's device. During implementation of this Service, we will gather information from you about your environment so that we can identify and deploy the appropriate commonly used scripts to improve the user experience.

(viii) Credential Guard (Enterprise Tier Only)

We will configure Windows Defender Credential Guard. This feature uses virtualization-based security to isolate Secrets so that only privileged system software can access them. Unauthorized access to these Secrets can lead to credential theft attacks, such as “pass-the-hash” or “pass-the-ticket. Windows Defender Credential Guard reduces the risks associated with these attacks by protecting NTLM password hashes, Kerberos “ticket granting tickets” and credentials stored by applications as domain credentials.

(b) Compliance Profiles

We will implement our standard, secure by design, Windows 10/11, Android, iOS and macOS compliance profiles in Microsoft Intune and assign these to all of your users and devices.

The standard compliance policy we implement will align, where available and applicable, your environment to the NCSC baselines and CIS Microsoft 365 Foundation Benchmark E3 Level 1 recommendations.

A report of your device compliance status against the policies we have assigned can be viewed in the Microsoft Intune admin centre.

Further information about the NCSC and CIS baseline recommendations can be found here:

Platform Guides - NCSC.GOV.UK

https://www.cisecurity.org/cybersecurity-best-practices/

We will configure a conditional access policy to report on non-compliant devices inside the Intune portal. Compliance reports will not be exported and sent to you as part of this Service. You can view all Intune reports directly from the Intune portal as you require.

(c) Windows Operating System Updates

For all tiers of this Service, it remains your responsibility to monitor the Microsoft update release schedule, plan and execute any required testing of systems and applications in your environment.

It is your responsibly to define the scope and complete all required testing of updates prior to the scheduled update date if required as part of your internal IT processes.

If you need an update to be deferred, you must raise a service request at least four (4) Business Days in advance of the scheduled update for the deferment to be guaranteed.

If you fail to complete any testing or to advise us that an update needs to be deferred, all updates will be automatically pushed out to your devices as detailed below.

Both Enterprise and Business tier, Windows updates will automatically be installed in accordance with the table below. If you have procured the Business Tier, we will

manually deploy and configure the update rings. If you have procured the Enterprise Tier, we will use Windows Autopatch to enable Microsoft to automatically manage the configuration of the updates:

	Pilot Ring	Preview Ring	Broad Ring	VIP Ring
Service Channel	Beta	Release preview	Retail	Retail
Quality Deferral	0	7 days	10 days	30 days
Feature Deferral	0	0	0	180 days
Update Release Date	Patch Tuesday (second Tuesday in the month)	Third Tuesday in the month	Third Friday in the month	The following month

Note: Feature Deferral is set to 0 as Feature Updates would automatically be deployed twice a year in accordance with the Feature Update policy deployed by us (unless you wish to remain on a specific Windows version, in which case it is your responsibility to notify us during Service Implementation).

As standard, we will create four (4) groups of devices in your Azure Active Directory:

- The pilot ring is for your IT staff to test bleeding edge features and ensure a general compatibility with the baseline hardware and software;
- The preview ring is for your key users across the business who will receive updates three to four weeks ahead of general release to test key line of business applications;
- The broad ring is for the remainder of your business; and
- The VIP ring is for business-critical machines. This should be used sparingly as it has the maximum deferral on both Quality Updates and Feature Updates.

If you have purchased the Enterprise tier, we will configure Microsoft's Autopatch service with the update schedule described above. Autopatch will automatically pause and resume updates should any issue be detected by Microsoft. You can find out more about Autopatch here:

What is Windows Autopatch? - Windows Deployment | Microsoft Learn

(d) Application Deployment Policies

We will package and assign the following in-scope third-party applications to all your users and devices:

(i) Microsoft 365 Apps (Outlook, Word, Excel, PowerPoint, Publisher, Access, OneDrive and Teams);

(ii) Microsoft Project and Visio using dynamic groups to auto install and uninstall on license addition / removal;

(iii) Microsoft Company Portal;

(iv) Microsoft To-Do;

(v) Browsers (Microsoft Edge); and

(vi) Basic Utilities (7-Zip).

Where supported by the applications, we will configure them to update automatically when new versions are released by the vendor(s).

You are responsible for ensuring you have purchased any required licences prior to using any third-party applications on your devices.

(e) Device Provisioning

(i) Windows Devices

We will configure Microsoft 365 to enable new Windows 10/11 devices to be configured automatically the first time they are turned on and logged onto by your end-users, anywhere in the world, provided that the device is connected to an active internet connection.

The devices will be provisioned with a business optimized Windows 10/11 Operating System.

You can preregister your devices for Autopilot in two ways:

(1) By asking your hardware supplier (“OEM”) to register the details of all new devices in your M365 tenant prior to shipping; or

(2) By manually collect the hardware identity of devices (hardware hashes) and provide this information to us in a comma-separated-value (“CSV”) file. At you request, we can perform this activity for you in accordance with Section 5.2.

For new users, you must provide us with a list of existing groups, applications and policies that you would like to be applied for that user and their devices at least five (5) Business Days before the user is due to receive their device. We will assign the user to your existing groups and policies in Azure AD according to the information you provide.

Changes to or creation of groups, AD policy rules or Intune packaged applications are not included in the scope of this Service.

All new devices will be Azure AD Joined only. For current devices, we can configure hybrid join using Azure AD Connect and Group Policies configuration with the machines being transitioned to Azure AD Joined when they require a rebuild or reach end-of-life.

If you provide us with a device naming convention, we will configure Autopilot to generate and assign device names automatically according to that convention.

(ii) Non-Windows Devices

Managed Apple devices must be enrolled to this Service by your IT team through Apple Business Manager following the guide we will provide you. The device will then provision using our compliance, application and configuration policies.

It is your responsibility to setup Apple Business Manager for your organisation following the guide we will provide you as we cannot do this for you. We will provide guidance as required.

Managed Android devices must be enrolled by your IT team to Managed Google Play by scanning the QR code we will provide you on a new or factory-reset device. The device will then provision using our compliance, application and configuration policies.

We will setup Managed Google Play for you and share the credentials with you as required to ensure smooth running of your Service.

Unmanaged Apple and Android devices must be enrolled by the end user who owns the device using the Microsoft Company Portal application and the guide we will provide. The supported applications on the device will then be managed by our Mobile App Protection policies as defined in Section 2.3.

(iii) Device Remote Wipe

For Managed Windows, iOS and Android devices, we will trigger a remote wipe of any device managed by Microsoft Intune at your request. This will wipe all user accounts, data, device management policies, settings and will reset the operating system to its default state and settings.

Please note that this feature is not applicable to macOS devices and unmanaged devices.

When we trigger the remote wipe and the command is received, the device will continually try to wipe itself until successful, including after a period of no power. This function ensures that the wipe action cannot be circumvented by turning off the device. Please note that whilst this process ensures a device is securely wiped, it could cause the device to cease to function properly or to be unable to reboot when turned off during the wiping process. For the avoidance of doubt, we will not be liable for such risk or any consequence of this activity where we wipe a device in accordance with your request.

You must not make any changes to your Active Directory prior to requesting a remote wipe from us. If you remove a user that has managed devices from Azure AD, we can no longer wipe or retire the devices associated with that user.

The remote wipe trigger will only be successful if the device is turned on and connected to the internet so that it can receive the command.

2.3 Microsoft 365 Mobile App Protection

(a) App Protection Policies

We will implement our standard, secure by design, mobile application management app protection policies. These policies define how your data, held in Microsoft 365, can be accessed and used on your users' unmanaged personal mobile devices through the official Microsoft Office mobile applications.

We will implement policies which enforce the Microsoft APP Data Protection Framework level 1 protections.

Further information about the Microsoft APP Data Protection Framework policies can be found at https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-framework.

Policies are only applied when apps are used in a work context on a mobile device. For example, when a user signs into an app with a work account or opens files that are stored in your organisation's OneDrive for Business.

After creating an app protection policy, the next time an assigned user opens one of the affected apps on a mobile device in a work context, the app will restart, notify them that it is now being managed by a policy, and will ask them to set up a PIN to access it.

Android users will be required to install the Microsoft Intune Company Portal app for Android on their mobile device.

(b) Remote Business Data wipe

At your request we can create a wipe request to remove company data from managed applications with application protection policies applied to them on mobile devices. This is limited to iOS/iPadOS and Android.

After we action your request and the remote business data wipe command is received by the mobile device, the next time the app runs on the device, company data will be removed from the app.

The remote data wipe trigger will only be successful if the device is turned on and connected to the internet/mobile network to receive the command.

2.4 Managed Microsoft Defender for Endpoint Service

Our Managed Microsoft Defender for Endpoint Service will be delivered as described in our Managed Microsoft Defender for Endpoint Service Description, which will be issued to you along with this Service Description when you purchase this Service.

Please note that our Managed Microsoft Defender for Endpoint Service will only be deployed on end-user endpoints managed by this Service in your environment.

For the avoidance of doubt, we will only be responsible for performing the activities set out in the Managed Microsoft Defender for Endpoint Service Description. We will not be liable for any threat or infection to your endpoints, or for any outcome of downtime caused by such threat or infection.

Any anti-virus solution in addition to the service described in our Managed Microsoft Defender for Endpoint Service Description is not included in the scope of this Service.

2.5 Asset List

Microsoft Intune admin center provides standard reports on the managed devices in your Microsoft 365 tenant including an asset list of all the enrolled devices.

We will provide you guidance on how to view the asset list in Microsoft Intune.

You will access these reports yourself as required directly in Microsoft Intune, following the guidance we have provided to you.

If you are having difficulty accessing these reports and would like us to provide you with an exported copy from Microsoft Intune, you can raise a change request in accordance with Section 5.2.

2.6 Platform Support

We will provide third line support for incidents raised by you related to the policies we have implemented in Microsoft Intune or Defender for Endpoint which cause repeatable impact to multiple users and cannot be resolved by your internal IT team(s). We will only accept and act on support incidents when raised by the users that you have nominated in your completed data capture form for this Service. You can nominate up to five (5) users (typically this would be your internal IT team).

We are only responsible to resolve issues with policies that we implemented, and which have not been changed by you. We reserve the right to charge you for the remediation steps that we have taken to resolve an incident if, during our investigations, we identify that you have changed a policy which we originally implemented for you without our approval. In these cases, we will notify you of the result of our investigation and provide you with details of the applicable Fees for incident resolution activities.

If you need bespoke policies in your Microsoft Intune environment in addition to the baseline we have implemented for you, you must provide us full documentation about these polices. Please note that the implementation and documentation of bespoke policies are not included in the scope of this Service. We will perform these activities as a professional service engagement subject to an additional Fee.

If you raise an incident with us and the root cause is identified as being a policy which you have created, our support teams will resolve the incident by disabling your policy. Please note that we do not support any policy that we have not implemented and documented in accordance with this Service Description. If you require an additional policy to be included in the scope of this Service, you must raise a service request with us, which would be subject to an additional Fee as set out in Section 5.2.

If we are unable to provide a fix or resolution steps for the incident to you, we will log a ticket with Microsoft and act as the intermediary between you and Microsoft until the ticket is resolved. We will provide you with status updates and request any pertinent information that Microsoft requires from you as part of its investigation.

You will provide end-user support for all third-party applications and for all first and second line end user requests and incidents.

You will investigate and resolve incidents which cannot be resolved by us via the Intune and Defenders portals, or incidents which require remote assistance or hands on remediation with the end-user or device.

You must not make any changes to any policies that we have implemented in your M365 tenant as part of your internal support processes or procedures. All incidents which require a change to a policy that we have implemented in your M365 tenant for you must be raised as an incident with us. We will implement such change following our standard change request process set out in Section 5.2 if the change complies with our security baseline.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
We will send you an introductory email along with a data capture form.	●	
You will provide us with the information requested in the data capture form.		●
We will send your nominated M365 Global Administrator (as specified in your data capture form) a CSP Reseller Relationship request link.	●	
Your nominated M365 Global Administrator will accept and approve the CSP Reseller Relationship request in your M365 Admin Portal.		●
If our delegated admin rights through the CSP Reseller Relationship prevent any implementation steps, we will create a Global Admin account in your M365 tenant for us to use to configure and monitor the features of this Service. This account does not require a M365 subscription assigned to it.	●	
If, due to your security settings, we are unable to create the Global Administrator account, you will create one for us and provide us with the login details.		●
You will setup Apple Business Manager for your organisation based on the guide we provide.		●
We will implement the features of this Service as detailed in this Service Description.	●	
You will manage end-user testing of the Service.		●
We will confirm the Ready for Service date.	●	

All implementation work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional fees for

any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

3.1 Ready for Service

The Ready for Service Date is the date when we (acting reasonably and properly) notify you that the implementation steps are complete and that the Service is ready for service. This date may be specified to occur at a later date, if mutually agreed to be so. If you consider that the Service is not ready for service on the date notified, you must notify us within two (2) weeks of our notification, after which the Ready for Service Date will be deemed to have occurred regardless of issues or defects of which you may later become aware and notify us about (which will then be dealt with as faults or service issues but will not change the Ready for Service Date).

4. Billing

The Service will be billed as Set-Up Fees and Recurring Fees as described in our Billing Guide using the definition of the Ready for Service Date in Section 3.1 of this Service Description, and as indicated in your Order Form.

We reserve the right to charge additional Fees in the following situations:

(a) Implementation work carried out outside Business Hours;

(b) Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA); and

(c) Any service request in excess of your entitlement set out in section 5.2 and any change request not specifically listed in section5.2.

5. Service Operations

You can log and track all of your requests using our client portal. We will provide you registration and login details will be provided during the Service Implementation phase.

Our support team can be contacted by phone, email or via our client portal and will be able to assist you with the following:

(a) Change requests;

(b) Incident management;

(c) Ticket updates;

(d) Portal logins; and

(e) General queries.

5.2 Service Request Entitlement

A service request for this Service is defined as one (1) request of the following items:

Service	Item
Create a new group in Azure AD	Create a new group of users or devices in Azure Active Directory.
Add a new device	Import a new device's hardware identity hash into Microsoft Intune and assign it to an existing group or user in Azure Active Directory.
Create a new user in Azure AD	Create a new user(s) in Azure Active Directory.
Add/remove device to a group	Add or remove a domain joined device to/from a group in Azure Active Directory.
Add/remove user to a group	Add or remove an existing user to/from a group in Azure Active Directory.
Device remote wipe	Initiate a remote wipe on a domain joined and Microsoft Intune managed device.
Asset list export	We will provide you with an exported report from Microsoft Intune of all devices enrolled in your Intune environment.
Import Autopilot CSV	Import a CSV file you provide us with hardware identities to preregister devices for Autopilot

As standard, we offer up to five (5) service request per month free of charge. We can implement additional service requests as and when required for an additional Fee which will be defined in your Order Form or SoW.

Any service request that is not specifically defined in the table above will be considered a professional services engagement subject to an additional Fee calculated on a time and materials basis.

We will implement standard service requests listed in the table above in accordance with the resolution times listed in our Operations Manual but, in any case, in no less that forty-eight (48) hours from receipt of the request. Please ensure to submit any urgent change, amendment or cancellation request at least forty-eight (48) hours prior the desired implementation date.

5.3 Monitoring

(a) Intune

We will monitor the update status of your Windows 10 and Windows 11 devices. If they fall outside of our supported N-1 version requirements and we are able to resolve the issue without your input, we will proceed with the resolution and you will not receive any notification. Where resolution requires us to contact you to assist in resolution, we will send a notification to your nominated contact(s).

Failure to respond within seven (7) days from when we send the notification will result in us forcing a restart of the Windows 10 and Windows 11 device to ensure it is using a supported version of the Windows Operating System. We will not be liable for any data loss or any impact that this action might have on your applications installed on your Windows 10 and Windows 11 device.

If our forced restart instruction fails to resolve the issue, we will block access from the non-compliant device via a Microsoft 365 Conditional Access policy and contact you to

discuss the joint steps required to remediate the problem and bring your device in line with our N-1 requirement.

6. Exit Assistance

As a standard, we will perform the following activities shortly before or upon termination of your Service:

(a) Suspend and cancel any Microsoft licences that you have purchased from us for the provision of this Service.

Please note that it is your responsibility to provide a valid termination notice in accordance with the terms of your MSA. We reserve the right to charge additional Fees for the performance of the activities listed above if you fail to provide such notice.

If you require us to perform any activities in addition to those listed above, we can provide professional services subject to an additional Fee.

7. Dependencies

We provide the Service subject to the following dependencies:

7.1 Client Obligations

(a) You will designate a project lead and technical contacts with the appropriate level of expertise to support the successful implementation and operation of the Service;

(b) You will provide us with all of the information and access to systems we require to complete the implementation and delivery of this Service;

(c) You will ensure our delegated admin permissions and enterprise app registration are not changed or removed from your M365 tenant while this Service is active;

(d) You will setup Apple Business Manager for your organisation following the guide we will provide you as we cannot do this for you;

(e) You will manage any of your own third parties needed during the implementation and operation of the Service;

(f) You will ensure that you have valid and current licences for all applications setup in your environment;

(g) You will not make any unauthorised changes in the Microsoft Intune, Azure Active Directory or Defender admin center pages in your M365 tenant;

(h) You will not make changes to any settings in the Intune and Defender administration portals while you have an active Service with us to ensure the stability of your environment. Please note that we actively scan managed environments for alignment and compliance to our policies. Any remediation of unauthorised changes that we perform will be subject to an additional professional services Fee;

(i) You will test all updates and alert us at least four (4) Business Days in advance of any scheduled update that you would like to be deferred;

(j) You will provide us with the required device information for all your existing and new assets so that they can be configured for management;

(k) You will be responsible for ensuring your existing end-user devices are configured correctly so that they can be enrolled into the endpoint management system. Please note that you may need to perform a complete wipe and rebuild of the operating system;

(l) It is your responsibly to define the scope and complete all required testing of updates prior to the scheduled update date if required as part of your internal IT processes;

(m) It is your responsibility to be aware of the Microsoft update release schedule and plan in your testing accordingly;

(n) You are responsible for ensuring you have purchased any required licence(s) prior to using any third-party applications on your devices;

(o) For new users, you must provide us with a list of existing groups, applications and policies that you want to be applied for that user and their devices at least seven (7) days before the user is due to receive their device;

(p) Where you need any bespoke policies, you will raise a chargeable change request with us in accordance with Section **Error! Reference source not found.**. Please note that t his change is outside the scope of this Service Description and is subject to an additional Fee;

(q) You will provide end-user support for all third-party applications;

(r) You will provide end-user support for all first and second line requests and incidents;

(s) You will investigate and resolve any patching / policy deployment errors which cannot be resolved by us via the Intune portal and require remote assistance or hands on remediation with the end-user device;

(t) You must not make any changes to any policies we have implemented in your M365 tenant as part of your internal support processes or procedures;

(u) If, due to your security settings, we are unable to create the Global Administrator account, you will create one for us and provide us with the login details;

(v) You will manage end-user testing of the Service;

(w) You must provide us with delegated admin access to your M365 tenant through a CSP reseller relationship so that we can implement the features of this Service;

(x) You must have all your existing users set up in or synchronised with Azure Active Directory.

8. Exclusions

The excluded items listed below are outside the scope of this Service Description:

(a) We will not perform proactive reporting. You can access Intune reports via the Intune portal at any time;

(b) Any configuration of your M365 tenant which is not directly related to the implementation of this service;

(c) Changes to conditional access policies after the Ready for Service Date;

(d) SCCM configuration or management;

(e) SCCM co-management configuration or management;

(f) Support for third-party integration with the core M365 application set;

(g) Backup of your data regardless of where it is stored;

(h) Updates, support and management of any policies that we did not create for you are not included in the scope for this Service;

(i) Support for bespoke services, macros or databases developed in the M365 application set; and

(j) Any other activities beyond those detailed in this Service Description.

This Service is designed to help you manage your M365 tenant and does not guarantee total protection against malware, virus and threats, or against security breaches or data loss (whether or not caused by the negligence of your users). Managed Microsoft Defender for Endpoint should be used as part of a wider approach to risk mitigation. For the avoidance of doubt, we will not be liable to you for any security breach or data loss in your M365 tenant.

We will not be liable for any malfunction or the performance of remediation activities if your devices cease to function properly or are unable to reboot after a wiping process that we perform in accordance with your request and as defined in Section 2.2(e)(iii).

Please note that certain policies or components associated with specific Service features are only available for specific devices. Please refer to the relevant Service feature description in Section 2 for specific exclusions.

9. Definitions and Acronyms

9.1 Definitions

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

The terms listed have the following meanings:

Term	Meaning
Apple Business Manager	A web-based portal for IT administrators to deploy iPhone, iPad, iPod touch, Apple TV, and Mac all from one place.
Autopatch	A cloud service that automates Windows, Microsoft 365 Apps for enterprise, Microsoft Edge, and Microsoft Teams updates to improve security and productivity across your organization.
Autopilot	Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use.
Azure Active Directory	A universal platform to manage and secure identities provided by Microsoft https://azure.microsoft.com/en-gb/services/active-directory/.
Azure AD Connect	Azure AD Connect (or also Azure AD Cloud Sync) is an application which runs on an on-prem server to synchronise your user identities between a traditional on-prem Active Directory Domain and an Azure Active Directory Forest.
Azure AD Joined	Azure AD joined devices are signed in to using an organizational Azure AD account. Access to resources can be controlled based on Azure AD account and Conditional Access policies applied to the device.
CIS Microsoft 365 Foundation Benchmark	As defined at https://www.cisecurity.org/benchmark/microsoft_365.
CSP Reseller Relationship	CSP is a relationship between you and Microsoft with a skilled partner in between. The partner will manage the subscription for you, which gives them more control over your customer experience and how you are billed
Company Portal	Microsoft Intune Company Portal application for Android devices.
Domain join	Windows Domain Join is a feature that lets users establish a remote and secure connection between their device and a work domain using credentials from the enterprise. The domain will have policies and settings defined within it and once a device is joined to it, the device will be bound to comply with the policies and settings issued to it.
Feature Deferral	The lead time applied to delay the deployment of a feature update
Feature Updates	Feature updates contain not only security and quality revisions, but also significant feature additions and changes.
Global Admin	The Global Admin role provides global access to most management features and data across Microsoft online services.
Group Policies	Group Policies are settings configured within Active Directory to control and manage your traditional Active Directory joined end-user machines and users.
Intune	Microsoft Intune Administrator Portal in Microsoft 365.
Kerberos	Kerberos authentication is a way to securely log in to a computer network. It involves the user requesting access, and the network sending back a "ticket" that proves the user's identity. The user's computer then uses this ticket to request access to specific services on the network, and the network checks that the ticket is valid before granting access. Kerberos is a widely used method for secure network authentication.
Microsoft 365	Microsoft 365 and Office 365 are cloud-based services designed to help meet your organization's needs for robust security, reliability, and user productivity. More information is available at https://support.microsoft.com/en-us/office/what-is-microsoft-365-847caf12-2589-452c-8aca-1c009797678b.
Microsoft 365 Conditional Access	Conditional Access is the protection of regulated content in a system by requiring certain criteria to be met before granting access to the content

Microsoft APP Data Protection Framework	App Protection policies protect your corporate data on unmanaged devices. The framework defines what policies should be in place. More information is available at Data protection framework using app protection policies.
Microsoft Intune	A tool to manage endpoint device configuration and policies. https://docs.microsoft.com/en-us/mem/endpoint-manager-overview.
Secret	Tokens, passwords, database connection strings, certificates, API keys, and other secrets.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.

9.2 Acronyms

Acronym	Meaning
AAD	Azure Active Directory
AD	Active Directory
CIS	Center for Internet Security
CSV	Comma Separated Value
M365	Microsoft 365
MACD	Move Add Change Delete
MAM	Mobile Application Management
MDM	Mobile Device Management
MSA	Master Services Agreement
NCSC	National Cyber Security Centre
NTLM	NT LAN Manager
O365	Office 365
OEM	Original Equipment Manufacturer
SoW	Statement of Work
SCCM	System Center Configuration Manager

10. Incident Classification Operational Targets

Incidents affecting the operation of our Windows 365 Service are classified using the service below:

		Scale			
	Impact Description	**Business Wide**	**Department**	**Team**	**Individual**
Business Impact	Critical impact – Not possible to complete key business tasks.	P1	P1	P2	P3
	High impact – Key business tasks are significantly degraded.	P1	P2	P3	P4
	Medium impact – Completion of key business tasks is made more difficult or taking longer.	P2	P3	P4	P4
	Low impact – The incident does not impact on business, or a workaround is available.	P3	P4	P4	P4

The associated response target below will apply based on the incident priority assigned.

	P1	**P2**	**P3**	**P4**
Response	30 mins	1 hour	2 hours	4 hours
Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days

11. Service Levels and Service Credits

11.1 Service Levels

The service levels associated with this service are detailed below:

Service	**Service Management Process**	**Metric**	**Target**
Response	Incident management	Service desk response times	90% within the published response target

11.2 Service Credits

There are no service credits associated with this service.