Contents

1. Service Overview

Our Windows 365 (“W365”) Service provides your licenced users with access to a Windows 365 Enterprise Cloud PC which is managed and secured by our baseline Intune and Defender for Endpoint policies. Each Cloud PC is assigned to your individual user and is their dedicated Windows machine.

W365 Cloud PC’s can be configured with either Windows 10 or Windows 11 operating systems. A complete list of the W365 Cloud PC configurations that we can provide (*e.g.* processor, RAM and storage) is available at https://docs.microsoft.com/en-us/windows-365/enterprise/cloud-pc-size-recommendations.

Our W365 Cloud PC’s are hosted in Microsoft’s UK South datacentre.

W365 Cloud PC’s can be accessed on internet connected devices through Microsoft supported Windows, macOS, Linux, Android and iOS remote desktop clients or through supported modern web browsers such as Microsoft Edge. Instructions for how to install and configure these clients will be available at https://windows365.microsoft.com/ when your Windows 365 Service is ready for service.

2. Service Specific Deliverables

2.1 Essential Licencing

Each of your users must have licenses for Windows 10/11 Enterprise E3, Intune, Azure AD P1, Defender for Endpoint (either Defender for Business or Defender for Endpoint P2) and Windows 365 to use their W365 Cloud PC.

You must have at least one (1) Microsoft 365 Business Premium or Microsoft 365 E3 licence assigned to each of your users to enable us to provide the monitoring features of this Service.

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 to use the W365 service. We can provide any additional licences that you require to be added to your Microsoft 365 tenant to enable this Service subject to a separate Fee which will be chargeable on a recurring monthly basis.

2.2 Windows 365 Enterprise Cloud PC

We will provision your W365 Cloud PCs in your Microsoft 365 tenant using a direct Azure AD join and the Microsoft hosted network.

We will provision your W365 Cloud PCs using the latest Windows 10 or Windows 11 gallery image provided by Microsoft.

We will install the latest version of the Microsoft 365 Apps on your W365 Cloud PCs.

For new users, you must provide us with a list of existing Azure AD groups, Intune packaged applications and policies that you would like to be applied to a user’s W365 Cloud PC at least four (4) days before the user requires access to their W365 Cloud PC. We will assign the user

and W365 Cloud PC to your existing groups and policies in Azure AD according to the information you provide.

2.3 Intune baseline

(a) Windows Operating System Updates

We will configure your W365 Cloud PCs to automatically install the Microsoft Quality Updates and Feature Updates for the Windows operating system including updates to Windows drivers.

As standard, we will create four (4) groups of devices in your Azure Active Directory: pilot ring, preview ring, broad ring and VIP ring. Each group will receive automatic updates at a different time to enable you to complete testing on a specific subnet of devices before the general release.

We will assign your devices to different rings in accordance with your instruction.

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 key users across your business who will receive updates three (3) to four (4) weeks ahead of general release to test key line of business applications. The broad ring is for the remainder of your business. The VIP ring is for business-critical machines and should be used sparingly and has the maximum deferral on both quality and feature updates.

Feature updates will automatically be deployed to all users at the same time when they are released by Microsoft every six (6) months. These have been tested by Microsoft before release to ensure no impact to the wide catalogue of frequently used applications.

We can uninstall feature updates and roll them back to the previous state for thirty (30) days after they are deployed in the event of an incident occurring.

We will deploy Quality and Features Updates for the Windows Operating System according to the table below.

Patch Management	Deliverable
Patching Frequency	Quality Updates are deployed according to update ring policy (see table below).
Patching Hours	24x7
Patching Days	Monday to Sunday
Patch Remediation	Updates can be uninstalled for a period of thirty (30) days.

The table below defines our standard approach:

	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).

(b) Configuration Profiles

We will implement our secure by design set of Windows 10/11 configuration profiles in Microsoft Intune and assign these to your W365 users and W365 Cloud PCs as appropriate.

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

The configuration policies that we will implement include policies which enforce your background image to be the same across all W365 Cloud PCs, user data to be automatically backed up to OneDrive for Business and a blank policy for configuring an Internet Explorer Enterprise Cloud Site List for any websites which require Microsoft Edge IE Mode.

For the avoidance of doubt, only data stored in the locations listed below will be automatically backed up to OneDrive for Business because of our configuration profile. 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:

(i) Desktop;

(ii) My Music;

(iii) My Documents;

(iv) C:\ProgramData\Microsoft\Windows\Start Menu\Programs;

(v) %APPDATA%\Microsoft\Windows\Start Menu\Programs;

(vi) %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar;

(vii) %APPDATA%\Microsoft\Signatures;

(viii) %LOCALAPPDATA%\Microsoft\Outlook\RoamCache;

(ix) %USERPROFILE%\Favorites;

(x) %USERPROFILE%\Links;

(xi) %APPDATA%\Microsoft\Excel\XLStart;

(xii) %APPDATA%\Microsoft\Word\STARTUP;;

(xiii) %LOCALAPPDATA%\Microsoft\Outlook;

(xiv) %APPDATA%\Microsoft\Templates;

(xv) %LOCALAPPDATA%\Microsoft\Office;

(xvi) %APPDATA%\Microsoft\Sticky Notes; and

(xvii) %LOCALAPPDATA%\Google\Chrome\User Data\Default.

(c) Compliance Profile

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

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

You can review a report of your W365 Cloud PC compliance status against the policies we have assigned in the Microsoft Intune admin centre.

2.4 Access to On-premises Resources

Should you require access to on-premises resources from your W365 Cloud PCs, we will configure Azure AD Cloud Trust to perform Single Sign-On (SSO) from Azure AD joined devices to traditional AD resources (when on-site or VPN connected). We will perform this activity as part of the Service Implementation phase if agreed with you and included in the scope of your SoW. Please note that this activity is subject to an additional Fee.

If you request our assistance to configure access to on-premises resources after the Ready for Service Date, we will perform this activity as a separate professional service engagement subject to a separate Fees.

You are responsible for ensuring your domain controllers are running Windows server 2016 or newer prior to us starting this work.

2.5 Defender for Endpoint Baseline

Our Defender for Endpoint baseline provides protection for your W365 Cloud PCs within your environment and monitors them for known and zero-day cyber threats to reduce your security risk. The Service provides 24x7 passive monitoring for alerts and incidents generated by the Defender for Endpoint and notification via a ticketed incident with additional information when your action is required to remediate a threat.

Where Microsoft Defender identifies attempted attacks and/or malicious activity, it automatically routes this information to our service desk, who will review and notify you via our IMS of any incidents that need to be addressed or may need further action.

If you require us to take additional action, either to continue to allow, deny, include and exclude the detected activity (if it has been identified by you as safe and as a legitimate process), you can raise a change request in accordance with Section 5.2.

Please note that incident analysis is not included in the scope of this Service. We are not liable for any outcome or downtime any threat may cause on the W365 Cloud PC.

In the event of any infection and where you need us to resolve the issue, we reserve the right to charge you for this service as a professional service, which will be billed on a time and materials basis.

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.		•
You will grant us sufficient permissions on your Microsoft 365 tenant to setup and support this service as advised by our engineers.		•
We will implement the features of this Service as detailed above in your Microsoft 365 tenant.	•	
You will manage end-user testing of the service.		•
We will confirm the Ready for Service date.	•	

Unless otherwise agreed with you, 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 in accordance with your MSA for any change in your requirements occurring after the implementation of the Service and outside the scope of the contract.

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 Windows 365 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 Recurring Fees monthly in advance and as one time Set-up Fees as described in the Billing Guide, using the definition of the Ready for Service Date in Section 3.1 of this Service Description.

5. Service Operations

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

Our 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.

When you contact our support team, we will issue you with a reference number which acts as your unique reference for your incident or request. We will ask you to quote this reference number when contacting the support team to provide information or an update.

5.1 Incident Management

If your users are unable to access the desktop of their W365 Cloud PC, you can log a ticket with our service desk.

During triage, we may adjust the ticket priority based on the incident classification definition in Section 9 and in accordance with our Operations Manual.

If we identify a problem at the platform level, which is managed by Microsoft, 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 notify you where Microsoft requires any pertinent information from you as part of its investigation.

Please note that support for the remote desktop clients' configuration on your endpoints is not included in the scope of this Service. Our investigation and resolution will be limited to ensuring that your end users can log onto and access their W365 Cloud PCs desktop through the latest version of the Microsoft Edge web browser.

Our resolution may include restarting or reprovisioning the W365 Cloud PC.

Successful access to the W365 Cloud PCs desktop will trigger your ticket to be closed. Please note that any change to your W365 Service that you require during the incident management process and that is not directly related to the restoration of the Service is out of scope.

If you require support outside of what is defined in this document, we will assist you in accordance with our standard support operating procedures as defined in our Operations Manual. Please note that if support is not requested according to our standard escalation procedures, there might be delays in response and resolution times.

5.2 Change Enablement

A change is defined as one (1) request of the following items:

Windows 365	Item
W365 Cloud PC	Provision a W365 Cloud PC using an existing provisioning policy to a new user by assigning them a W365 license user and adding them to an existing Azure AD group.
	Deprovision a W365 Cloud PC.
	Reassign a W365 Cloud PC and licence to a different existing user in Azure AD.
	Assign existing applications in Intune to a W365 Cloud PC.
	Assign an application uninstall policy to a W365 Cloud PC or existing Azure AD group which contains multiple existing W365 Cloud PCs for an existing application in Intune.
	Assign or remove a user from an existing group in Azure AD.
	Reset a W365 Cloud PC.
	Resize a W365 Cloud PC to a new size where an appropriate licence is available in your M365 tenant.
	Reprovision a W365 Cloud PC.
	Restore a W365 Cloud PC from an automated restore point.
Intune Baseline	Modify an existing operating system update schedule.
Defender for Endpoint Baseline	Modify ‘allow’ and ‘block’ listings.
	Modify scan timings.
	Detected threat activity responses: allow, deny, include and exclude.
Information Requests	Any request for an exported report of data which is available from the Microsoft Intune admin portal.

As a standard, we offer up to five (5) changes per month free of charge.

We can implement additional changes as and when required for an additional Fee which will be defined in your Order Form or SoW. Any change request that is not specifically defined in the table above will be deemed out of scope and delivered as a professional services engagement subject to an additional Fee calculated on a time and materials basis. These changes must follow the process covered in our MSA. Please note that we reserve the right to increase your Fee should you require changes to the scope of your Services.

We will implement standard changes listed in the table above in accordance with the resolution times for priority 4 tickets as listed in Section 9.

Information requests will be treated as change requests. Only the information requests specifically included in the table above will be considered in scope and deducted from the monthly allowance.

5.3 Monitoring

(a) Intune

We will monitor the update status of your W365 cloud PCs. If they fall outside of our supported N-1 version requirements and this can be resolved without notification, we will do this. 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 reprovisioning the W365 Cloud PC to ensure it is using a supported version of the Windows Operating System.

We are not responsible for any data loss or any effect that this action might have on your applications installed on your W365 Cloud PCs.

(b) Defender for Endpoint

We will monitor the incidents generated by Defender for Endpoint. We will issue a notification to your nominated contact(s) based upon the incident information received.

When alerts generated from Defender for Endpoint require further action by you, we will raise these as incidents and manage them as defined in Section 5.1. An automated ticket will be sent to your nominated contact(s) email address.

Please note that end user support is outside the scope of this Service.

You are responsible for providing us details of your nominated contact(s), which may include your own internal support team, a third-party support team or our service desk (if you have procured a separate managed service with us as indicated on your Order Form and at an additional Fee).

This Service does not provide a comprehensive incident management solution. If an issue which has generated an alert or incident is not resolved by your nominated contact(s) within twenty-four (24) hours from when we sent the notification, we reserve the right to disable alerting and further notifications for that issue and we will not be liable for any impact to your organisation as a result of that issue.

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; and

(b) Deprovision all W365 Cloud PCs.

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 Windows 365 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 are responsible for installing the relevant Windows 365 client on your endpoints as required;

(d) You will not make any unauthorised changes in the Microsoft Intune, Azure AD or Defender for Endpoint admin centre pages in your M365 tenant while this service is live;

(e) You are responsible for all end user testing after operating system updates;

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

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

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

(i) You understand that no data should be stored solely on the W365 Cloud PC's hard drive. It is your responsibility to ensure all your end users' data is synchronised to network or cloud storage such as Microsoft OneDrive to prevent data loss should the W365 Cloud PC need to be restarted or reprovisioned;

(j) You are responsible for ensuring that your domain controllers are running Windows Server 2016 or newer prior to requesting us to configure access to on-premises resources from your W365 Cloud PCs; and

(k) You are responsible for ensuring all applications installed on your W365 Cloud PCs are using a vendor supported version and that you have purchased all required licences for such applications.

7.2 Prerequisites

(a) You must have an existing Microsoft 365 tenant;

(b) You must have the licences listed in Section 2.1; and

(c) You must have setup all required users in Azure AD.

7.3 Service Dependencies

(a) To setup your initial environment, one of your users with global administrative rights will need to complete our web form and grant an Enterprise App Registration access to the tenant.

7.4 Exclusions

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

(a) Support for remote desktop clients on your endpoints;

(b) Support and management of applications installed on top of the operating system;

(c) End user desktop support;

(d) Capacity management;

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

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

(g) Packaging and installation of third-part applications on your W365 Cloud PCs;

(h) Updates, support and management of any policies that we did not create;

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

(j) We are not responsible for any security breaches within your environment or W365 Cloud PCs relating to any patching or lack thereof;

(k) We are not responsible for any effect that the updates might have on your applications installed on your W365 Cloud PCs;

(l) We do not guarantee the end user performance of the Windows 365 Service environment; and

(m) Any activities other than those specifically noted in this Service Description.

8. Definitions and Acronyms

8.1 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
Azure AD Cloud Trust	Azure AD Cloud Trust uses Azure AD Connect to create additional attributes within your on-prem Active Directory to allow Single Sign-On to on-prem resources via an Azure AD joined device.
Enterprise App Registration	Enterprise App Registrations are a mechanism for programmatic access to your Azure and Intune environment with pre-configured permissions.
Feature Deferral	The number of days after the release of a feature update before it installs onto devices.
Feature Update	Feature updates are a Microsoft term for updates which are released twice per year, around March and September. As the name suggests, these will add new features to Windows 10, delivered in bite-sized chunks compared to the previous practice of Windows releases every 3-5 years.
Internet Explorer Enterprise Cloud Site List	As you transition your workflows and applications from IE11 to IE mode, Cloud Site List Management lets you manage your site lists for IE mode in the cloud.
Intune	As defined at https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune.
CIS Microsoft 365 Foundations Benchmark E3 Level 1	As defined at https://www.cisecurity.org/benchmark/microsoft_365.
Microsoft Edge IE Mode	IE mode on Microsoft Edge makes it easy to use all of the sites your organization needs in a single browser. It uses the integrated Chromium engine for modern sites, and it uses the Trident MSHTML engine from Internet Explorer 11 (IE11) for legacy sites.
Quality Deferral	The number of days after the release of a quality update before it installs onto devices.
Quality Update	Quality update is a Microsoft term for updates which deliver both security and non-security fixes. They are typically released on the second Tuesday of each month, though they can be released at any time. Quality updates include security updates, critical updates, servicing stack updates, and driver updates.
Service Channel	Servicing channels are the first way to separate users into deployment groups for feature and Quality Update.
Single Sign-On	Single sign-on is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.

Windows 365 Enterprise Cloud PC (or “Cloud PC”)	As defined at https://docs.microsoft.com/en-us/windows-365/enterprise/overview.

8.2 Acronyms

Acronym	Meaning
Azure AD	Azure Active Directory
CIS	Center for Internet Security
IMS	Integrated Management System
NCSC	National Cyber Security Centre
SoW	Statement of Work
SSO	Single Sign-On
VPN	Virtual Private Network
W365	Windows 365
W365 Cloud PC	Windows 365 Enterprise Cloud PC

9. Incident classification and 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

10. Service Levels and Service Credits

10.1 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

10.2 Service Credits

There are no service credits associated with this service.