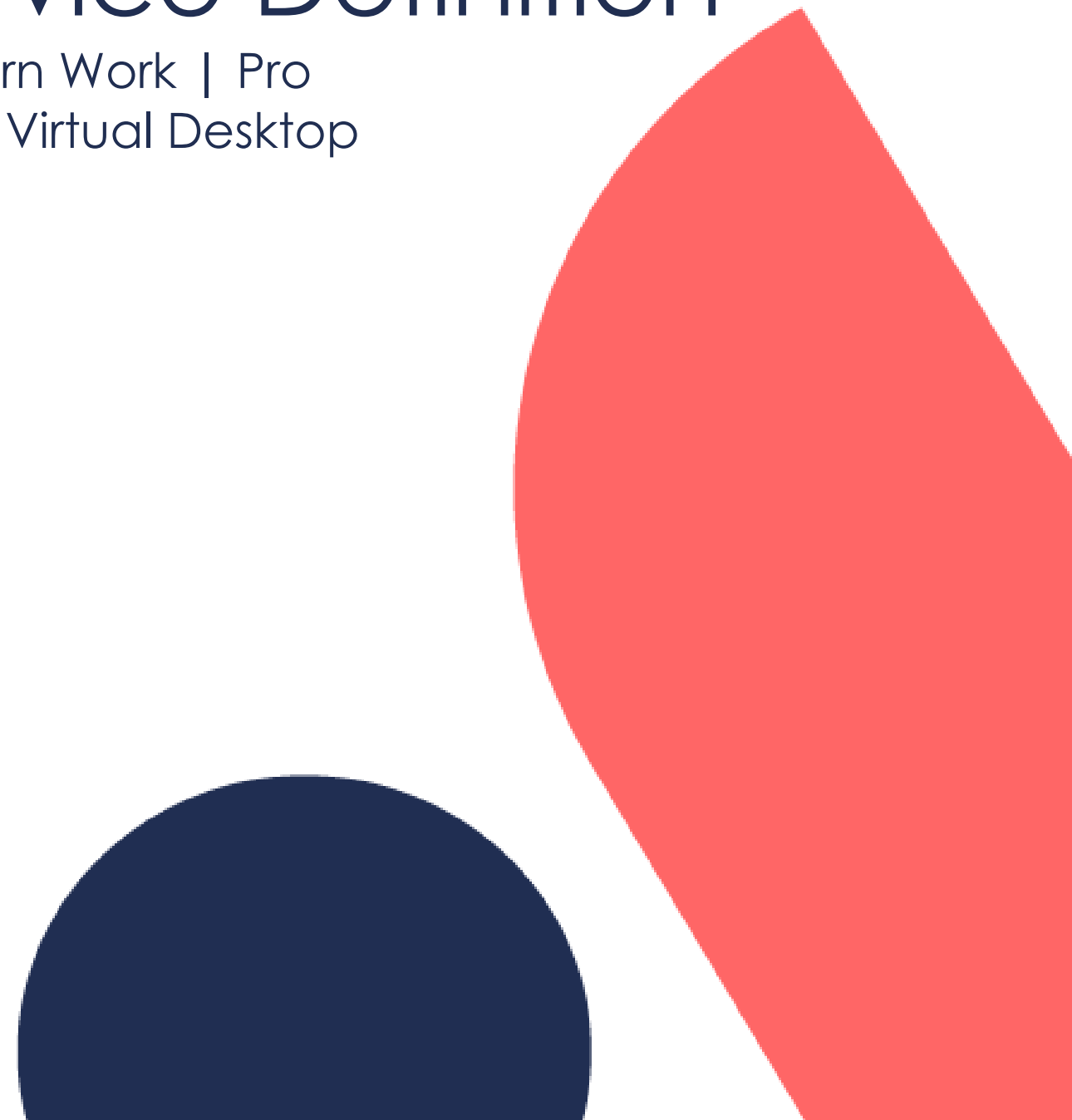
Service Definition

Modern Work | Pro
Azure Virtual Desktop



Product Terms for Azure Virtual Desktop Pro Package

The following Product Terms apply if the relevant Services are included within your Quotation in the event of a conflict between the Product Terms and the applicable Terms and Conditions, these Product Terms shall prevail, but only to the extent of such conflict. Any capitalised terms used in this document shall have the meanings set out in the applicable Terms and Conditions (save where expressly provided otherwise below) and any additional definitions outlined below shall also apply.

1. Service Definition Overview

The Azure Virtual Desktop (AVD) Pro Managed Service offered by ANS is designed to provide comprehensive support and management of your AVD infrastructure.

This service is structured to seamlessly integrate with your existing IT service delivery model and is delivered by ANS' 2nd, 3rd line support, and Operations Center Team (centralised service responsible for continuously monitoring the performance and health of services).

2. Pre-Requisites

To onboard and deliver this service optimally, certain pre-requisites must be met. ANS's Delivery Team will work closely with you to ensure these requirements are fulfilled.

These pre-requisites are:

- An existing IT service delivery capability (who provide first line support to end users). For a full list of expected existing IT delivery responsibilities, please refer to the "*Azure Virtual Desktop Base Support RACI Matrix*" for the full RACI (Responsible, Accountable, Consulted, Informed) Matrix. However, some examples include:
  - Configuration and maintenance of User Outlook
  - Management and maintenance of Local peripherals (E.g. Printer)
- Global Administrator Role and Subscription Owner Permissions for ANS Delivery Team
- GDAP Administrative Access Permissions for ANS Technical Support Engineers
- Registered Partner Admin Link

3. Operational Services

3.1. Operations Description

ANS provide a Service Desk function (accessible by telephone and via ANS Portal) to provide support services to authorised Customer Personnel.

Normal Business Hours = 8:00 -20:00, Monday to Friday (excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

3.1.1. Service Desk Contact Details

The Service Desk can be contacted via:

Telephone	**0800 923 0617**
Priority Support System	https://portal.ans.co.uk/pss
Emergency Out of Normal Business Hours	0800 231 5995

Additional contact details (where available) can be found within the ANS Portal.

3.2. Operations Baseline

Service	Service Description	Service Hours
Incident Management		
Telephone and Remote diagnostics for faults	Fault diagnostics to troubleshoot platform faults via: • Telephone • Remote Connection	Normal Business Hours
Service Desk – Non-Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Suppliers Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4).	Normal Business Hours
Service Desk – Business Critical Faults	The Supplier provides 24/7 access with relevant phone contact details to the Suppliers Service Desk for critical system down scenarios (P1) only.	24 x 7
Session Host Triage and Troubleshooting	The Supplier shall investigate and resolve incidents relating to the AVD Session Hosts. If the issue is application or user specific, this will be passed back to the Customers existing IT Service Delivery Team.	24 x 7
Storage Triage and Troubleshooting	The Supplier investigates and resolves platform incidents relating to storage components.	24 x 7
Priority Escalation to Vendor	Priority escalation to vendors.	Normal Business Hours

High Priority Escalation to Vendor	High Priority escalation to vendor for Priority 1 business critical faults.	24 x 7
Image Security Management	The Supplier shall deploy Microsoft Defender on Gold Images upon solution deployment. The Supplier shall translate security alerts and provide a remediation action point for the customer. The supplier shall only perform infrastructure effecting action points.	Normal Business Alerts
Service Request Management		
User Creation and Deletion	The Supplier provides access to self-service functionality for new user creations and user deletions.	24 x 7
Desktop Branding	The Supplier shall support existing IT service delivery to implement desktop background and screensaver personalisation (Where available, exclusions apply).	Normal Business Hours
Two Factor Authentication	The Supplier shall implement Two Factor Authentication for AVD users utilising Microsoft's conditional access policies (where available, exclusions apply). The supplier shall work with existing service delivery function to ensure it is working optimally.	Normal Business Hours
Self-Service Password Resets (SSPR)	The Supplier shall implement and maintain SSPR polices to ensure password efficient password resets (Where available, exclusions apply).	Normal Business Hours
Backup File Restore	The Supplier shall complete requested backup restores from a given directory.	Normal Business Hours
Change Management & Advisory		
Session Host & Host Pool Management	The Supplier shall action change requests to session host configuration.	Normal Business Hours
Storage & Profile Management	The Supplier shall action change requests to storage configuration, including FSLogix. The supplier shall also provide guidance and advice around self-service changes to Storage configuration.	Normal Business Hours
Power Management and Auto-Scaling	The Supplier shall review change requests to auto-scaling changes. The supplier shall inform the customer of the potential impacts before implementing.	On Request
Operating System (OS) Patch Management	The Supplier shall patch customer images and in-scope additional servers in line with the agreed schedule (Monthly or Quarterly).	Normal Business Hours
Zero Day OS Patching	The Supplier provides Zero Day Patch release service in the event of an urgent zero-day patch released to infrastructure.	Normal Business Hours
Image Management	The Supplier shall only manage the OS version and patch levels. Manual Image release to AVD Host Pools is restricted to twice per calendar month. Self-Service releases are unlimited.	Normal Business Hours
Control Plane Management	The Supplier shall host and maintain appropriate patch levels on ANS' infrastructure control plane (outside of customer subscription), to aid correct functionality of self-service tooling.	Normal Business Hours
Backup Setup & Configuration	The Supplier shall configure backups to the agreed specification. The Supplier shall action change requests to modify the initial configuration.	Normal Business Hours
Line-of-Business Server Management	The Supplier shall manage up to 5 additional virtual machines (VMs) that support the customers AVD desktop application workloads. This brings the VMs in scope of the Patching, OS, Backup management	

	described above. Additional requirements outside this can be managed by ANS Managed Database or Cloud Service.	Normal Business Hours
Network Configuration management	The Supplier shall review and fulfill proposed network configuration changes to the AVD environment	Normal Business Hours
Monitoring & Event Management		
Platform Monitoring	The Supplier will monitor the platform infrastructure providing thresholds, availability, and performance.	24 x 7
Session Host Monitoring	The Supplier will monitor the AVD platform session hosts providing bespoke dashboards, thresholds, availability, and performance.	24 x 7
Monitoring Response	The Supplier shall action monitoring tickets (where relevant) on behalf of the customers. Required changes will be presented to the customer for approval.	Normal Business Hours
Backup Tooling & Monitoring	The Supplier will monitor for back up failures.	24 x 7
Governance, Cost Management & Optimisation		
Continuous Documentation	The Supplier will deliver automatic generation of cloud environment diagrams, including resources and their dependencies	On Request
User Login Report	The Supplier shall deliver user login activity reports. The reports will only encompass the data included in the specified retention period for Event Logging.	On Request
Asset Register	Cloud Resource asset register collected continuously for all cloud-based assets within accounts under ANS service.	On Request
Event Log	Continuous event log collection of all actions performed on cloud platform through GUI, API or automation.	24 x 7
Consumption Insights Report	Consumption Insight Reporting will be distributed at regular intervals. The Report will cover the previous period and be based on available data dimensions.	Normal Business Hours
Cost Reporting	The Supplier shall provide Self-Service access for the customer to keep track of spend.	24 x 7
Cost Optimisation	The Supplier shall ensure the customer is utilising the appropriate compute cost optimisation strategies (Reserved Instances, Savings Plans and Hybrid Benefit where available).	Normal Business Hours
Price to Performance Review	The Supplier shall conduct a Bi-Annual Price to performance review of AVD subscription(s) in scope to highlight potential financial savings. This is upon request.	Normal Business Hours
Overall Cost (Per User) Transparency Reports	The Supplier Shall provide a Bi-Annual Cost per user transparency Report upon request.	Normal Business Hours
Insider Program	The Supplier shall include the customer in the early access release of new AVD features.	On Request
Service Operations		
Customer Portal Access	Customer access to ANS Portal providing visibility of all Service-related tickets, billing information, and self-service access (where available).	24 x 7
Self-Service	The Supplier provides access to self-service functionality where platform functions can be	24x7

	managed by existing IT service delivery function. This includes: - Session Host/Host Pool Management - File/App/DB Server Management - Image Management - Storage Management - Network Management - Backup Policies	
Knowledge Base	The Supplier shall provide access to the Knowledge Base including UAT guidance documentation.	24 x 7
Admin Training	The Supplier shall provide Admin Training via E-learning, Videos and the Knowledge Base.	24 x 7
Account Management	The Supplier shall provide an Account Manager.	Normal Business Hours
Emergency Changes	Following a Critical Incident, the Supplier will implement Emergency Changes.	24 x 7

4. Incident & Request Management

An Incident is "An unplanned interruption to the IT service or a reduction in the quality of the IT service." Incidents have a wide scope and can fall into different classification and prioritiation levels. In contrast, a request is a "pre-defined, pre-authorised request from a user for something to be provided." While incidents deal with needs, requests deal with wants.

In the event an incdent or request is raised, the service desk will ensure it is logged and categorised before triaging using the Incident and Request Classification process. Incidents can be classified into 4 categories. These are Critical (P1), High (P2), Normal (P3) and Low (P4). Due to the generally lower priority of requests, they are mostly classified as High, Normal and Low. Each category of classification has an SLA for Response time and Agreed Resolution.

4.1. Incident and Request Criticality Classification

A Critical (P1) incident is a large-scale outage that requires both parties to commit to working together to restore services as quickly as possible. In the Pro Azure Virtual Desktop Service, the scope for a Critical (P1) incident is:

- Every user unable to log in
- Every user with sessions disconnected
- FSLogix failure to attach for all users
- Infrastructure or Network failure

A High (P2) Incident or Request is a time sensitive service affecting task or issue impacting at least 25% of users. The scope for a High (P2) Incident or Request includes:

- Login Issues impacting over 25% of users
- Degraded desktop performance impacting over 25% of users or 5 users
- Application Server Outage or degraded performance

A Normal (P3) Request is a task or issue that is non-time critical or has a lower business impact. The scope for P3 Request includes but not limited to:

- VM capacity limits
- Password Resets
- Granting access to an application
- Creation and Deletion of Users
- Network Changes and Requests
- Granting Access to files and folders
- Desktop configuration Requests
- Restores from Backups
- All other standard changes that are pre-defined and pre-agreed. These are normally initiated by a user or an authorised representative of a user.

A Low (P4) Request is a task that is not time bound or is a general query. There is no SLA for a Low (P4) Request.

4.1.1. Incident Priority Table:

The information above is simplified and displayed visually in the table below:

Effect	Business/Potential Impact (% of numbers of user impacted)			
	Minor / Subset (<25%)	Moderate / Majority (>25 - <50%)	Major / All (>50%)	Application/File/ Database VM
System Down	P1			
Degraded Performance	P3	P2		
Singular User Issue	P3		P2	P3
General and Queries	P4			

4.2. Incident & Request Response

For an Incident, "Response" is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, ANS Portal update, telephone call or in person. For a detailed process flow, please refer to the Handover Documentation. The "Agreed Resolution" is the time from when the ticket is first logged to ANS agreeing a solution or temporary workaround with the service user.

Priority	Response SLA	Notification Frequency	Agreed Resolution
Critical (P1)	2 Hours	1 Hour	4 Hours
High (P2)	4 Hours	4 Hours	8 Hours
Normal (P3)	8 Hours	1 Day	2 Days
Low (P4)	2 Days	N/A	N/A

From the time of Response until resolution, updates shall be provided to the Named Contacts through ANS Portal updates at such frequencies as set out in the table above.

There is no limit on the number of support requests, but excessive usage (beyond acceptable use policy) will be investigated by the Company and future requests may be chargeable. Typically support requests taking in excess of 3 hours to implement will be chargeable. Charges for excessive usage or tasks requiring longer implementation times will be calculated at our standard hourly rate.

5. Service Level Targets

Category	Service Level Target
P1 Incidents	100% of Incidents responded to within 2 Normal Business Hours
P2 Incidents	100% of Incidents responded to within 4 Normal Business Hours.
P3 Incidents	100% of Incidents responded to within 24 Normal Business Hours.
P4 Incidents	100% of Incidents responded to within 48 Normal Business Hours.

ANS will endeavour to complete all tickets within these timeframes. If an SLA is missed, the customer will be eligible for service credits (50% of a day's managed service for every hour in breach of SLA). Please note, service credits only apply to missed Agreed Resolution SLAs.

6. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Agreement should be consulted.

For the purpose of these sections "Customer Supported Assets" means the Cloud solution provided by AWS or Microsoft (as the case may be) to the Customer and in relation to which ANS is providing the support more particularly outlined in these Product Terms.

"Demarcation Zone" means infrastructure or solutions not being Customer Supported Assets.

a. Issues resulting from misconfiguration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets.
c. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets.
d. End User or 1st Line support.
e. Technical Advice to any persons not listed as a Named Contact.
f. Failure to meet SLA due to Public Cloud provider outages.
g. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges.
h. Emergency Changes that are not a direct output of a P1 incident may be subject to Additional Service Charges e.g., poor planning from a Customer Managed Project.
i. Incident & Change Management refers only to platform issues and configuration requests.
j. Application patching will not be managed by the Supplier.
k. Support of images not UAT tested by the Customer.
l. Migration or deletion of data.
m. Application Streaming/MSIx App Attach Support.
n. Configuration, management and back up of SQL databases.
o. Incident Management of issues stemming from endpoint incompatibility or network availability.
p. Implementation or maintenance of on-premises peripherals. E.g., Printers.
q. Single Sign-On (SSO) Implementation or management.

r. Support on Azure resources outside of the Customer Supported Assets.
s. Disaster recovery or backup restores for testing purposes.
t. Implementation of Two-Factor Authentication with Third-Party Identity providers.

7. Customer Responsibilities

Including but not limited to:

a. The Customer shall have an established end user support function that may be validated by the Supplier.
b. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed.
c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
    a. Affected Services.
    b. Business Impact.
    c. Number and type of users affected.
    d. Recent changes on Supported Assets (regardless of perceived impact).
d. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed.
e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have Supplier recommended hardware and vendor support in place.
f. The Customer is responsible for all configuration backups outside of the Supported Assets without exception.
g. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process.
h. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Modern Work Managed Services Handbook.
i. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier).
j. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions.
k. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
l. It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business-Critical Incidents raised via email.
m. Operating System level/Application support will be required by the Customer.
n. Customer will be responsible for all UAT testing of image deployments.

8. Assumptions

a. All Customer Supported Assets and Azure Accounts within the Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels.
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date.
c. All Customer specific pre-requisites have been completed before contract commencement.
d. The Customer will provide a suitable specification platform for the Enterprise Monitoring collector server.
e. The Customer has an existing IT Service Delivery Team in place to support with End-Users.
f. The Customer will provide resource to work with the Supplier to on-board the service.
g. The Supplier reserves the right to cap the number of resources that are classified as Customer Supported Assets to 5 excluding those configured as part of the core Azure Virtual Desktop solution.

9. Partner Admin Link

ANS' Managed Cloud for Azure incorporates Microsoft Signature Cloud Support for any issues that require escalation to Microsoft. In order for this to be able to be fulfilled, Microsoft leverage information collected from the Partner Admin Link (PAL) system to assign back-end support rights. As such ANS must be registered as the digital PAL on any Subscriptions that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the PAL and must have either Owner or Contributor rights to all subscriptions and resources that contain or contribute to assets under support or management for the entire duration of this agreement.