Service Description

Modern Workplace Advance Managed Service
August 2025

transparity

Contents

1. Service Overview

The Modern Workplace Managed Service – Advanced includes support and a range of proactive services for Microsoft 365 based solutions.

2. Service Features

The following is a high-level overview of the functionality available within this service:

KEY:

● Inclusive as part of the standard service offering

◒ Inclusive and as standard when you have purchased the relevant service or if you have requested service(s) that have been documented in your SoW

○ Available as an optional upgrade for an additional fee.

Feature	Advanced
24/7 Incident Response	●
Transparity Adoption Portal	●
Service Requests	●
Service Management and Reporting	●

2.1 24/7 Incident Response

For incidents within your Microsoft 365 environment, we will provide 24/7 incident response, if the incident relates to the services provided by the Microsoft, we will escalate to Microsoft.

We will follow the Target Response as defined in section 8.1 of this service description.

2.2 Service Requests

The managed service includes five (5) service requests per month for non-project related work within your Microsoft 365 environment.

2.3 Service Management

As part of your account team, you will be allocated a Service Delivery Manager. They will serve as your primary contact(s) for day-to-day management and interaction for this Service. In addition, the Service Delivery Manager will act on your behalf to ensure we adhere to our processes and standards to meet contracted obligations and provide advice and guidance on your Microsoft 365 Service.

The responsibilities and/or deliverables of your allocated Service Delivery Manager will include the following as outlined in the table below: -

Name	Description	Frequency	Forum
Operational Risk Management and Tracking	An operational repository (including the Risk Register) will be created for all risks identified and will include information about each risk, e.g., the nature of the risk, reference, and owner, as well as any mitigation	Quarterly	Service Review

Name	Description	Frequency	Forum
	measures. This report will be reviewed with you via Service Delivery Manager at your service reviews.		
Continual Service Improvement Advice	Strategic advice based on intelligence provided by the Service to investigate how we can potentially increase the quality of products and services at a minimal cost for you. This advice will be tracked in a Continuous Service Improvement plan owned by the Service Delivery Manager. This will be reviewed with you via Service Delivery Manager at your agreed service reviews.	Quarterly	Service Review
SLA Breach and Complaints Management	We provide support including graphical information and narrative to you.	As and when an Incident occurs	Service Review
Risk Register	We maintain a register of all known risks for ongoing management – please refer to the Operational Risk and Management Tracking above.	As and when a risk occurs	Service Review

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

3.1 Transparity Control Centre

As part of this service, we will provide you with access to the Transparity Control Centre[1]*, the portal includes the following functionality: -

Feature	Description
Overview Dashboard	Licencing overview, including seat count
Renewals Dashboard	Upcoming renewals
Self-Service	Self-service portal for purchasing additional license SKU's
Billing	Access to your Microsoft 365 invoices

4. Billing

4.1 Additional Charges

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

- Implementation work carried out outside Business Hours; and
- Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

[1] This portal is only available for customers who purchase their Microsoft 365 licencing through Transparity.

5. Dependencies

We will provide the service subject to the following dependencies:

- All professional services required to set up this Service will be subject to separate Statements of Work and Charges and, where applicable, Service Descriptions.

5.1 Customer Obligations

- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company ("Nominated Contacts"). They will be the designated people with whom all contact is made regarding all requests.
- You will provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling. For example:
  - Microsoft's Partner Admin Link (PAL);
  - Microsoft Granular Delegated Access Permissions (GDAP) relationship;
  - Microsoft 365 Lighthouse relationship and delegations;
  - Service Principals;
  - Administration break-glass accounts; and
- For Microsoft 365 subscriptions not purchased through our CSP we will not be able to raise incidents with Microsoft unless you have purchased a separate Microsoft support agreement;
- You will allow us to deploy infrastructure in each public cloud region to handle the collection of activity and diagnostics logs into our monitoring platform.
- You will actively work with our operations team to resolve any raised incidents or Service Requests, or any activities relating to patching, that require your input or action. For example, you may be required to make any required changes to an end user device to which we have no access.
- Some incidents may require user-impacting remediation activity. You are responsible for distributing and coordinating end-user communications and activity unless agreed otherwise during the planning of the activity.
- It is your responsibility to comply with your data sovereignty controls, policies, and procedures.

5.2 Service Restrictions

- We will provide and support the Service on a reasonable endeavours basis only and will not be subject to any availability targets, if:
  - the OS residing on your end user device is out of vendor support, or
  - no support contract with the OS provider is in place, or
  - the end user device is configured in direct contravention of the requirements, best practices, or specific guidelines for support.
- When a ticket is opened with Microsoft the Transparity SLA is paused until a response is received from the Microsoft
- We reserve the right to defer or reschedule any planned changes in the event a Critical Incident investigation prevents this. Critical Incident Response will always take priority over Monitoring Alerts and tasks that can be deferred.

6. Exclusions

- End user support is excluded from this service.
- Microsoft Entra ID (formerly known as Azure Active Directory) or Microsoft Windows Active Directory either in your Supported Public Cloud Platform or any other location is excluded from this Service;
- The implementation or configuration of new technology is not included within the Service. Where this applies your Account Manager will present our recommended approach in a costed proposal for your approval
- Identified risks will be logged into our risk register. We will always seek to work with you on these risks and have you approved them where you do not wish or are not able to remediate the item. If we are unable to contact you in a timely manner or if you delay approval of the risk, the risk will be logged and automatically approved on your behalf. These open risks will form part of the ongoing monthly report for you to review.
- In the event that you fail to adopt recommendations or progress active risk register items raised during the execution of the service our ability to provide the service may be diminished. Should this lead to a material reduction in the quality of the service we can provide, we reserve the right to terminate the Service. Your Service Delivery Manager will highlight and seek to progress issues falling into this category; liaising with you and your Account Manager to identify and communicate corrective actions necessary to maintain the service before such action is taken.

6.1 Third Party Related

- Managing incident maintenance for:
  - 3rd party systems,
  - Software, and/or
  - SaaS services
- Specifically, if the above items are not covered by a third party's warranty, support agreement, or terms of use.
- Management, configuration, maintenance, administration of third-party appliances, Customer applications, and any code used to create, update, or deploy applications from third parties or by the Customer is excluded from this Service;
- Certificate management is limited to platform services. Certificate renewals or management on server or end user devices is not in scope.

7. Definitions and Acronyms

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

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
CSP	Cloud Solution provider
GDAP	Granular Delegated Access Permissions
OS	Operating System
PAL	Partner Admin Link
PaaS	Platform as a Service
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SoW	Statement of Work
VM	Virtual Machine
VPN	Virtual Private Network
WAR	Well Architected Review

8. Service Level Agreement and Operational Targets

8.1 24*7 Incident Response

	P1	P2	P3	P4
Hours of Support	24*7 Monday – Sunday	24*7 Monday – Sunday	08:00-18:00 Monday – Friday	08:00-18:00 Monday - Friday
Response	15 mins	Four (4) hours	Eight (8) hours	Twelve (12) hours

8.2 Incident Prioritisation

Priority	Severity	Description
P1	Critical	**Business service outage** • System/Service/Application down or unhealthy. Extremely urgent • Very high impact in all business areas, extreme impact on multiple users and disruption is excessive, such as Cloud platform failures, Virtual Machine failures and Cloud networking or connectivity failure • Business critical - work cannot continue
P2	High	**Business service impaired** • High impact on significant business areas or specific users • Individual user cannot complete high priority/business-critical work, or department or group of users unable to continue with routine work • Business critical - work is impaired

Priority	Severity	Description
P3	Medium	**Group of users affected** • Platform or application problem – user or group priority work cannot be completed • A group of users are experiencing system or business application
P4	Low	**One (1) person affected or minor service fault** • Minor system or application error • Backup or Patching Failure • An individual user is experiencing system or business application problems but is still able to work
P5	Routine	**Non-urgent investigations** • General advice and guidance or agreed scheduled activity