# Microsoft Azure from Dell Service Description

## Introduction

Dell is pleased to provide you with the Microsoft Azure Cloud Services from Dell (the "Service(s)") in accordance with this Microsoft Azure Service Description ("Service Description"). Your quote, order form or other mutually-agreed upon form of invoice or order acknowledgment (as applicable, the "Order Form") will include the name of the Subscription(s) and available service options that you purchased. Unless you have a separate written and signed master agreement that explicitly authorizes the sale of these Services, the Services and this Service Description are governed by the Dell Cloud Solutions Agreement located at Dell.com/cloudterms. For additional assistance or to request a copy of your applicable agreement(s), contact Dell technical support or your sales representative.

## The Scope of These Services

A complete list of the Services covered by this Service Description can be found in Appendix A. Dell's responsibilities include:

**Provisioning.** Dell will utilize the Microsoft Azure Management portal or other interfaces to create the Azure Active Directory tenant(s) and Subscription(s) on your behalf.

**Support.** Dell will provide 24x7 support in English for Subscription(s) purchased from Dell (see Appendix A for eligible Azure Services). Support is provided through the Standard plan (included at no additional cost) and paid Managed Services plans (see Appendix A for details). Support questions regarding the performance of Azure Services may be re-directed by Dell to Microsoft for resolution. Any issues regarding your on-premise infrastructure, architecture, appropriate service usage, or ongoing operation of Azure Services may be re-directed to Dell's managed services and/or consulting teams for engagement at an additional fee. If you are interested in these services, you may email Get_Azure@dell.com.

The Azure Services are more fully described at https://azure.microsoft.com ("Azure Services"). Service Level Agreement ("SLA") describes Microsoft's commitments for uptime and connectivity for Azure Services. These SLAs can be found at: https://azure.microsoft.com/en-us/support/legal/sla/. Dell's Azure Support Plans are more fully described in Appendix A.

## Your Responsibilities

You will be responsible for:

- Training staff to a minimal level of competency on Azure Services, feature configuration, and maintenance.
- Administrative functions for Microsoft Entra ID (Azure Active Directory) related to Azure Services purchased from Dell.
- Maintenance of on-premise infrastructure.



Internal Use - Confidential

- Recovery of on-premise infrastructure in the event of an outage, including restoring data and applications from the Azure Services.
- Ensuring that when a P1 or P2 incident is identified, you phone the toll-free number provided to ensure response and restoration are as quick as possible and business impact is minimized.
- Logging P3 or P4 incident and service request tickets via the agreed support process.
- Providing approval to change service requests prior to work commencing.
- Participating in Problem Management activities and making reasonable endeavors to minimize the volume and complexity of incidents.
- Reasonable availability of your representative(s) when Dell is restoring a Service-related incident or service request.
- Advanced scheduling of all Service-related service requests and other special Services.
- Maintaining current documentation of your Azure environment and notifying Dell of any changes through the agreed change management process.

**Authority to Grant Access:** As your Cloud Solution Provider, Dell is required by Microsoft to provide first-line technical support for your Azure environment. To deliver this support, and to ensure you receive the full benefits of the CSP program, you must grant Dell Granular Delegated Administration Privileges (“GDAP”). GDAP provides secure, role-specific, time-bound access to your tenant aligned with Zero Trust principles. You may review or revoke access at any time from the Microsoft 365 Admin Center.

**Definitions.** For purposes of this Section: "Managed Subscription" means each Azure subscription transacted or billed by Provider for Customer under the Microsoft Cloud Solution Provider ("CSP") program, including subscriptions created, added, or transferred into Provider's billing during the term. A subscription ceases to be a Managed Subscription upon its removal from Provider's CSP billing, provided that such removal does not constitute a departure triggering the Partner Transfer Fee under this Service Description. "Required Access" means standing Azure role-based access control ("RBAC") assignments at the scope of each Managed Subscription, in either of the following configurations: **(a)** the default administrative assignment created automatically when Provider provisions a Managed Subscription, under which Provider's admin agent group holds the Azure built-in role "Owner" as a foreign principal (i.e., an identity from Provider's Microsoft Entra ID tenant granted role assignment in Customer's tenant); or **(b)** where Customer elects by written notice to replace configuration (a): the Azure built-in role "Contributor" assigned to Provider's engineering security group or service principal, and the Azure built-in role "Support Request Contributor" assigned to Provider's support desk security group, each as identified by Provider in writing, each at subscription scope. In either configuration, Required Access must be standing: not subject to expiration, time limits, activation steps, or approval workflows. Standing access is required for Provider to deliver the automated monitoring, incident detection, optimization recommendations, and Service Level commitments described in this Service Description. "Eligible Consumption" means Customer's Azure consumption on the affected Managed Subscriptions invoiced at pay-as-you-go meter rates, excluding reservation and savings plan purchases, usage covered by reservations or savings plans, spot virtual machine usage, and Marketplace or other third-party charges. Eligible Consumption is the basis for calculating the Reduced-Access Delivery Fee described below.

**Access obligation.** Customer will maintain Required Access continuously on every Managed

Subscription and will provide at least ten (10) business days' written notice before removing or modifying any component of it. Granular delegated admin privileges (GDAP) enable Provider sign-in for directory-level tasks only; the presence, absence, or expiry of GDAP does not affect this Section, and its absence limits only those directory-level tasks. For the avoidance of doubt, this Section governs Azure subscription-level RBAC access required for Provider to deliver managed services, automated monitoring, and the Service Level commitments described in this Service Description. Directory-level access via GDAP is governed separately under the 'Authority to Grant Access' section of this Service Description. Removal of GDAP does not affect the obligations in this Section, and removal of Required Access under this Section does not affect the obligations regarding GDAP. If Customer removes or modifies Required Access without providing the ten (10) business days' written notice required above, the Reduced-Access Delivery Fee described below applies retroactively from the date of actual removal as determined by Azure activity logs.

**Effect of removal.** If Required Access is removed or reduced on any Managed Subscription, then from the date of removal until restoration: **(a)** service levels for the affected Managed Subscriptions, including the escalation service level, are suspended, and Provider will deliver Support Services on a reasonable-efforts, advisory-only basis; **(b)** a Reduced-Access Delivery Fee equal to fifteen percent (15%) of Eligible Consumption on the affected Managed Subscriptions applies, reflecting the increased cost and reduced automation of delivering services without standing access and the service delivery model on which Customer's plan is based; the Fee is waived in full if Required Access is restored within five (5) business days after Provider's written notice of the removal; **(c)** any preferential consumption discount conditioned on the managed delivery model is suspended for the same period, provided the combined effect of (b) and (c) does not exceed fifteen (15) percentage points of Eligible Consumption. The Reduced-Access Delivery Fee and SLA suspension under this Section do not apply where Required Access is lost due to (i) Microsoft-initiated changes to the Azure platform, Azure RBAC service, or Partner Center that prevent Provider from maintaining the Required Access configuration; (ii) termination of Customer's Azure subscription by Microsoft pursuant to the Microsoft Customer Agreement; or (iii) a force majeure event as defined in the applicable master agreement. For the avoidance of doubt, the Reduced-Access Delivery Fee applies only during periods in which Customer remains a Dell CSP customer and Required Access is not maintained. Upon Customer's notification of departure triggering the Partner Transfer Fee under this Service Description, the Reduced-Access Delivery Fee ceases to accrue from the date of the departure notification. The Partner Transfer Fee is calculated based on the remaining Partner Commitment Period from the date of departure notification and is independent of any Reduced-Access Delivery Fee previously invoiced. The Reduced-Access Delivery Fee is not credited against, deducted from, or offset by the Partner Transfer Fee, and the Partner Transfer Fee is not credited against, deducted from, or offset by the Reduced-Access Delivery Fee.

**Third Party Warranties.** These Services may require Dell to access hardware or software that is not manufactured by Dell. Some manufacturers' warranties may become void if Dell or anyone else other than the manufacturer works on the hardware or software. Customer will ensure that Dell's performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Customer. Dell does not take responsibility for third party warranties or for any effect that the Services may have on those warranties.



Internal Use - Confidential

## Supplemental Terms & Conditions Applicable to Cloud & SaaS Services

**1. Term of Service.** This Service Description commences on the date listed on your Order Form and continues through the term ("Term") indicated on the Order Form. As applicable, the number of systems, licenses, installations, deployments, managed end points or end-users for which you have purchased any one or more Services, the rate or price, and the applicable Term for each Service is indicated on Customer's Order Form.

**2A. Payment for Hardware Purchased With Services.** Unless otherwise agreed to in writing, payment for hardware shall in no case be contingent upon performance or delivery of cloud or SaaS services purchased with such hardware.

**2B. Optional Services.** Optional services (including point-of-need support, installation, consulting, managed, professional, support, security or training services) may be available for purchase from Dell and will vary by your location. Optional services may require a separate agreement with Dell. In the absence of such agreement, optional services are provided pursuant to this Service Description.

**2C. Assignment.** Dell may assign this Service and/or Service Description to qualified third party service providers.

**2D. Geographic Limitations and Relocation.** This Service is not available at all locations. Service options, including service levels, technical support hours, and on-site response times will vary by geography and certain options may not be available for purchase in your location, so please contact your sales representative for these details.

**2E. Liability.** DELL WILL HAVE NO LIABILITY FOR:

- ANY OF YOUR CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION;
- LOST OR CORRUPTED DATA, PROGRAMS OR SOFTWARE;
- DAMAGED OR LOST REMOVABLE MEDIA;
- THE LOSS OF USE OF A SYSTEM OR NETWORK; AND/OR
- FOR ANY ACTS OR OMISSIONS, INCLUDING NEGLIGENCE, BY DELL OR A THIRD-PARTY SERVICE PROVIDER.

Dell will not be responsible for the restoration or reinstallation of any programs or data.



Internal Use - Confidential

# Appendix A

## Azure Cloud Services from Dell – Support Plans

### Introduction

Dell is pleased to provide Support Plans ("Support Plan(s)") for Azure Services. Every Azure Service covered by this Service Description includes the Standard support plan at no additional cost. Customers seeking proactive management, compliance governance, cost optimization, and dedicated account management may subscribe to one of three paid Managed Services plans: Advanced, Premium, or Enterprise.

### Scope of Support

Support Plans purchased from Dell will be administered by Dell Azure support representatives, and include the following:

- User support. Provide support for frequently asked questions, set-up & usage, general best practices, and billing & invoicing.
- Product support. Provide support when the Azure Services are not working as expected or the service stops working.
- Services support. Respond to your inquiries with information on any service interruption, relay expectations, as available from Microsoft, on when the system will be back online.

### Issue Resolution Process

For Azure Services support, you may call (888) 649-4090 or email AzureCSP_Support@Cloudstore.dell.com. Issue resolution will follow established steps, in order:

- Level 1 and Level 2 support. Dell technical support agents/engineers will be utilized for troubleshooting.
- Level 3 support. When appropriate, cases will be escalated to Microsoft support by Dell technical support agents.

*Support is available via (888) 649-4090 or AzureCSP_Support@Cloudstore.dell.com for all plans. Service levels and response times are applied based on your active Support Plan.*

*24/7 P1/P2 break-fix support is provided through our L1/L2 Technical Support team. Managed Services engineers are available during business hours and are engaged for P1 escalations as needed.*

## Exclusions

For the avoidance of doubt, the following activities are not included in the scope of this Service Description and apply to all plans, including the Standard plan and all paid Managed Services plans:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The development of any intellectual property created solely and specifically for you.
- Support for Azure Services not purchased from Dell and not listed in Appendix A.
- Configuration of features within Azure Services, such as frequency of back-ups, or size and performance of virtual machines (VMs), unless included in a paid Managed Services plan.
- Networking, other than the specific Services covered by this Service Description.



Internal Use - Confidential

- Performance or availability issues due to factors outside Dell's reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to the Microsoft data centers, including at your site or between your site and the Microsoft data center).
- Performance or availability issues that result from the use of services, hardware, or software not provided by Dell, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services.
- Azure Sentinel SIEM management.
- On-Premises Active Directory, Office 365 and any Desktop applications.
- Application-layer monitoring, support or integration, observability tool configuration and management. Governance and optimization activities are limited to platform-level configuration and do not include application code changes, debugging, or data-pipeline logic.
- Operating System and infrastructure not deployed to cloud standards.
- Management and administration of operating systems and infrastructure including OS and Infrastructure Patching.
- Management of any non-cloud native tools or solutions (e.g., backup appliance or network appliance management).
- Networking rules setup and configurations and network topology and diagrams.
- SOC and SIEM services.
- Security breach Incident Management.
- The management and optimization of the specific workloads, services, or applications running on the Public Cloud Platform (e.g., the code or data pipelines in Databricks, or the applications within containers).
- Custom software development.
- Project management.
- Consultancy, implementation, configuration or operations of 3rd party systems or software.
- Physical datacenter related activities, such as implementation, testing and/or fixing of network equipment, servers, power units or cables.
- Azure services from another partner vendor.
- Creation of Azure implementation and deployment plans.
- Custom scripting.
- Creation of a digital recovery plan.
- Application recovery assessment and readiness for Azure Site Recovery.
- Testing of site failover.
- Remediation after failover testing.
- User access management.
- Line of business workloads running within a virtual instance whether on-premise or in the public cloud, unless otherwise specifically indicated as supported by Dell.
- Third-party products, applications or services obtained through the Microsoft Azure Marketplace or directly from another vendor.

**Out-of-Scope Work.** If you require services, tasks, or activities that fall outside the scope of this Service Description, including but not limited to custom implementations, consulting engagements, migrations, or specialized project work, please contact your Dell Azure account team at Get_Azure@dell.com. Out-of-



Internal Use - Confidential

scope work may be delivered under a separate, custom Statement of Work with agreed scope, timeline, and pricing. Any such Statement of Work will be governed by your applicable master agreement with Dell (Commercial Terms of Sale or separately executed master services agreement)

This Service Description does not confer any warranties which are in addition to the warranties provided under the Terms or your separate written master agreement with Dell, if applicable.



Internal Use - Confidential

## Part 1: Standard Plan (Included at No Additional Cost)

The Standard plan is the foundational level of support included with every Azure Service covered by this Service Description. It was formerly known as the Premium support plan. Every Dell Azure CSP customer receives the Standard plan automatically.

### What's Included in the Standard Plan

- Unlimited 24x7 break/fix technical support for P1 and P2 incidents through online submission.
- Business hours support (8AM–5PM US Central Standard Time, Monday–Friday) for P3 and P4 incidents.
- <3 hour maximum initial response time for P1 service incidents.
- Callback phone support (up to three times a month).
- Access to the Azure Status dashboard at https://azure.microsoft.com/en-us/status/.
- Access to Azure forum resources at https://azure.microsoft.com/en-us/support/forums/.
- Full access to the Surveil FinOps platform for cost visibility and optimization insights.
- Subscription management (does not include user administration).
- Maximum Microsoft Severity A issues.

The Standard plan also includes initial setup assistance for Azure Cloud Backup Services, consisting of the following:

- Azure Backup – includes on-premise files, folders, and system states by using the Microsoft Azure Recovery Services (MARS) agent. As well as on-premises VMs (Hyper-V and VMware) and other on-premises workloads using the Azure Backup Server (MABS).
- File Recovery – restore SQL Database, individual files, folders, and VMs in Azure or on-premises.
- Azure Site Recovery – replicating an Azure VM to a different Azure region directly from the Azure portal that can be used for disaster recovery.

### What's NOT Included in the Standard Plan

The Standard plan is a reactive, break/fix support plan. The following capabilities are not included and are only available through a paid Managed Services plan:

- Proactive monitoring of cloud resources, CIS benchmark compliance checks, or ITSM alarm integration.
- Compliance reporting against NZISM, SOC2, CIS, or any other framework.
- Cost optimization reports or recommendations.
- Custom Surveil governance policies (Surveil access is included; custom policy setup is not).
- Dedicated project hours for configuration changes, recommendations, or improvements.
- Technical Account Manager or priority escalation.
- Workload maintenance, architecture reviews, or sprint participation.
- Entra ID monitoring, Conditional Access reviews, PIM governance, or access reviews.
- Azure Virtual Desktop (AVD) management.
- Dev/Test subscription governance.
- Proactive onboarding of new Azure GA services.
- Monthly calls, Quarterly Business Reviews, or scheduled reporting cadence.



Internal Use - Confidential

## Part 2: Managed Services Plans (Paid)

Customers seeking proactive management beyond the Standard plan may subscribe to one of three paid Managed Services plans. Each tier builds upon the previous, providing increasing depth of coverage, compliance, governance, and dedicated account management. To be eligible, you must be a Microsoft Cloud Service Provider (CSP) Azure plan customer.

*Note: Everything included in the Standard plan (Part 1) is also included in all paid Managed Services plans below. The features listed here are in addition to what you already receive with the Standard plan.*

### Project Hours — General Rules (All Paid Plans)

The following rules apply to all included project hours across Advanced, Premium, and Enterprise plans:

- Project hours can be used for action outcomes that are part of the recommendations from monthly reports.
- Project hours are dedicated to Engineer time. TAM hours are separate and cover account management, reporting, cost and governance functions, and priority escalation.
- Up to 50% of unused project hours may be carried forward to the following month. Carried-forward hours expire at the end of that month and cannot be carried further. Upon expiry or non-renewal of a paid Managed Services plan, any accrued or carried-forward project hours are forfeited without refund, credit, or compensation.
- Issues initially reported as incidents that are determined to be configuration requests, how-to questions, or consulting work will be fulfilled using your included project hours. Dell will notify you prior to reclassifying an incident as consulting or configuration work and consuming project hours. If you dispute the reclassification, you may raise the dispute with your Dell Azure account team for a review. Pending resolution, the project hours in question will not be consumed.
- All project hours are allocated based on engineer availability and scheduled on a first-come-first-served basis. Advanced scheduling is recommended to ensure availability.
- All reporting is provided in Dell's standard reporting format. Custom reporting formats or custom reports utilizing native Azure Services are not included.

### Resource Scope Baseline

Upon onboarding to any paid Managed Services plan, you and our engineering team will jointly define the in-scope Azure resources for monitoring ("Resource Scope Baseline") within 10 business days. If the Resource Scope Baseline is not agreed within 10 business days, Dell will monitor all Azure resources within subscriptions active under your Dell CSP account at the time of onboarding, and the parties will continue to work in good faith to finalize the baseline. Changes to the agreed Resource Scope Baseline require written agreement between authorized representatives of both parties, which may be evidenced by email confirmation.



Internal Use - Confidential

### Advanced Plan

The Advanced plan is the entry-level paid Managed Services plan, designed for customers with growing Azure footprints who need foundational monitoring, compliance checks, and a small allocation of dedicated project hours.

#### *What's Included in the Advanced Plan*

**Everything in the Standard plan, plus:**

**Support**

- 5 included project hours per month for action items from monthly reports.
- Unlimited callback phone support.

**Monitoring & Security**

- Daily automated CIS Benchmark Compliance checks with monthly report.
- Cloud resource monitoring across the agreed Resource Scope Baseline.
- ITSM alarm integration with managed alert rules and action groups.
- Basic Entra ID health monitoring.
- Compliance standards: CIS only.

**Cost & Governance**

- Full Surveil platform access (same as Standard).
- Monthly cost optimization summary report.
- Monthly written report.

**Specialized Workloads**

- New Azure Services (GA): assessed and prioritized as engineering capacity permits, without a committed timeline. We will prioritize new GA services based on relevance to your environment.

#### *What's NOT Included in the Advanced Plan*

- Compliance standards beyond CIS (no NZISM, SOC2).
- Custom Surveil governance policies.
- Proactive least-privilege audits.
- Quarterly Conditional Access reviews or full Entra ID lifecycle management.
- Workload maintenance, architecture reviews, or sprint participation.
- Azure Virtual Desktop (AVD) management.
- Dev/Test subscription governance.
- Technical Account Manager or priority escalation.
- Monthly call or Quarterly Business Review (written report only).



Internal Use - Confidential

### Premium Plan

The Premium plan is designed for mid-market customers with compliance requirements and production workloads that need proactive maintenance, broader compliance coverage, and deeper governance.

#### *What's Included in the Premium Plan*

**Everything in the Advanced plan, plus:**

**Support**

- 10 included project hours per month (double the Advanced allocation).

**Monitoring & Security**

- Quarterly Conditional Access review for Entra ID.
- Compliance standards expanded to: CIS, NZISM, and SOC2.
- Proactive least-privilege audits and recommended remediation.

**Cost & Governance**

- Custom Surveil policy setup and ongoing maintenance.
- Monthly call in addition to monthly written report.

**Proactive Operations**

- Workload maintenance for efficiency, security, and Azure WAF compliance.
- Lifecycle management of in-scope workloads via runbooks and Logic Apps.

#### *What's NOT Included in the Premium Plan*

- Technical Account Manager or priority escalation (Enterprise only).
- Annual architecture review (Enterprise only).
- Sprint participation (Enterprise only).
- Azure Virtual Desktop (AVD) management (Enterprise only).
- Dev/Test subscription governance (Enterprise only).
- Full Entra ID lifecycle management including PIM, access reviews, auto-offboarding (Enterprise only).
- 90-day SLA for new Azure GA services (assessed and prioritized as capacity permits only).
- Quarterly Business Review (Enterprise only).



Internal Use - Confidential

### Enterprise Plan

The Enterprise plan is the most comprehensive Managed Services plan, designed for complex, large-scale Azure environments with multi-region deployments, AVD, mature identity lifecycle requirements, and the need for a dedicated account manager.

#### *What's Included in the Enterprise Plan*

**Everything in the Premium plan, plus:**

**Support**

- 30 included project hours per month.
- Named Technical Account Manager (TAM) as your dedicated point of contact. TAM hours are separate from included project hours and cover account management, reporting, cost and governance functions, and priority escalation.
- Priority escalation through your TAM.

**Monitoring & Security**

- Full Entra ID lifecycle management (Conditional Access, PIM, access reviews, auto-offboarding workflows).

**Cost & Governance**

- Quarterly Business Review in addition to monthly call and written reports.

**Proactive Operations**

- Annual structured Architecture Review (Well-Architected Review aligned).
- Sprint participation including planning, backlog refinement, and retrospectives. Sprint Participation activities consume included project hours.

**Specialized Workloads**

- Dev/Test subscription governance including tagging, policies, budgets, and auto-start/stop.
- Azure Virtual Desktop (AVD) full management: host pools, scaling, image management, UX monitoring. AVD management activities consume included project hours.
- Full Entra ID lifecycle workflows: auto-offboarding, role revocation, access reviews.
- New Azure Services (GA): 90-day SLA for onboarding (upgraded from capacity-based scheduling).

#### *What's NOT Included in the Enterprise Plan*

The Enterprise plan is the highest tier of Managed Services and is subject to the same exclusions listed in the Exclusions section of this Service Description.



Internal Use - Confidential

## Support Plan Comparison — All Plans at a Glance

*The Standard plan (formerly known as Premium) is included at no additional cost with every Azure Service covered by this Service Description. Advanced, Premium, and Enterprise are paid Managed Services plans available for separate purchase.*

| | Standard (Included) | Advanced (Paid) | Premium (Paid) | Enterprise (Paid) |
|---|---|---|---|---|
| **SUPPORT** | | | | |
| Unlimited 24x7 subscription and billing inquiries | Yes | Yes | Yes | Yes |
| Access to Azure Status dashboard | Yes | Yes | Yes | Yes |
| Access to Azure forums | Yes | Yes | Yes | Yes |
| Triage of non-Microsoft technologies running on Azure[1] | Yes | Yes | Yes | Yes |
| Unlimited 24x7 break/fix technical support[2] | Yes | Yes | Yes | Yes |
| SLA Response (P1) | < 3 hours | 3 hours | 3 hours | 3 hours |
| Maximum Microsoft severity[3] | A | A | A | A |
| Business Hours Support (P3/P4) | Yes | Yes | Yes | Yes |
| Callback phone support | 3/month | Unlimited | Unlimited | Unlimited |
| Included Project Hours | — | 5 hrs/mo | 10 hrs/mo | 30 hrs/mo |
| Technical Account Manager | — | — | — | Named TAM |
| Priority Escalation | — | — | — | Via TAM |
| **MONITORING & SECURITY** | | | | |
| CIS Benchmark Compliance | — | Daily checks | Daily checks | Daily checks |
| Cloud Resource Monitoring | — | Agreed scope | Agreed scope | Agreed scope |
| ITSM Alarm Integration | — | Yes | Yes | Yes |
| Entra ID Monitoring | — | Basic health | Quarterly CA review | Full lifecycle mgmt |
| Compliance Standards | — | CIS only | CIS, SOC2, NZISM | CIS, SOC2, NZISM |
| Least-Privilege Audits | — | — | Proactive | Proactive |
| Proactive monitoring of incidents | — | — | — | Severity A incidents |
| **COST & GOVERNANCE** | | | | |
| Surveil Access | Full access for Azure CSP subscriptions managed by Dell | Full access for Azure CSP subscriptions managed by Dell | Full access for Azure CSP subscriptions managed by Dell | Full access for Azure CSP subscriptions managed by Dell |
| Cost Optimization Reports | — | Monthly summary | Monthly summary | Monthly summary |
| Custom Surveil Policies | — | — | Setup & maintenance | Setup & maintenance |
| Reporting Cadence | — | Monthly report | Monthly call | Quarterly QBR |
| **PROACTIVE OPERATIONS** | | | | |
| Workload Maintenance | — | — | Efficiency, security, WAF | Efficiency, security, WAF |
| Architecture Review | — | — | — | Annual WAR |
| Sprint Participation | — | — | — | Planning & review |
| **SPECIALIZED WORKLOADS** | | | | |
| Dev/Test Subscriptions | — | — | — | Full coverage |
| Azure Virtual Desktop (AVD) | — | — | — | Full management |



Internal Use - Confidential

| | | | | |
|---|---|---|---|---|
| Entra ID Lifecycle | — | — | — | CA, PIM, access reviews |
| New Azure Services (GA) | — | As capacity permits | As capacity permits | 90-day SLA |

[1]Multiple non-Microsoft technologies run on the Azure platform, e.g., Linux, Oracle, and SAP. Dell Azure support representatives will help in isolating the issue between the Azure Service and the non-Microsoft technologies. Full technical support will be provided if the issue is determined to be caused by an Azure Service. In the case that an adequate solution to your issue is not achieved, you might be referred to other support channels that are available for the non-Microsoft technologies.

[2]Based on support availability of 24x7 in English for all severities.

[3]The incident severity is the Microsoft degree of business impact (https://support.microsoft.com/en-us/gp/azuresevdetails).

## Service Levels (Paid Managed Services Plans)

The following Service Levels apply to all paid Managed Services plans (Advanced, Premium, Enterprise). Standard plan incidents are handled via Dell's existing Azure L1 & L2 Technical Support with best-effort response times.

### Incident Priority Definitions

| Priority | Description |
|---|---|
| **P1 — Critical Business Impact** | Total failure of the primary functions of a Core Business Service or Core Technical Service. A security breach resulting in non-authorized access. A high impact environmental incident. |
| **P2 — Major Business Impact** | Partial failure or degradation of the primary functions of a Core Business Service or Core Technical Service; or critical failures with an acceptable workaround in place. |
| **P3** | A failure where a single User cannot access the primary functions of a Service. Partial failure or inhibited performance of non-Core Business Services impacting multiple Users. |
| **P4** | Non-urgent incident with minor impact; restoration can be scheduled at a time agreed with User. Incidents relating to DR, development or test environments. |

### Incident Service Levels

| Priority | Response Time | Restoration Time |
|---|---|---|
| P1 | 90% within 3 hours | 90% within 4 hours |
| P2 | | 90% within 8 hours |
| P3 | | 90% within 3 Business Days |
| P4 | | 90% within 5 Business Days |

### Service Request Service Levels

| Priority | Response Time | Fulfilment Time |
|---|---|---|
| P4 — Standard | 90% within 1 Business Day | 80% within 5 Business Days; 100% within 10 Business Days |
| P5 — Non-standard / Complex | 90% within 2 Business Days | 80% scoped within 5 Business Days; 100% scoped within 10 Business Days |
| P5 — Pay as you go | 90% within 2 Business Days | 80% scoped within 5 Business Days of commercial approval |

The Service Level targets set forth in this Service Description are performance objectives. Dell will use commercially reasonable efforts to meet the stated targets. In the event Dell fails to meet a Service Level target, your sole and exclusive remedy shall be to escalate the matter to your Dell Azure account team for corrective action.

### Service Level Measurement Methodology

- Response Service Levels: elapsed time from when Dell or management tool has raised the ticket to when the ticket is assigned and accepted by a resolver group.



Internal Use - Confidential

- Restoration/Fulfilment Service Levels: elapsed time from ticket creation to restoration of an incident or fulfilment of a service request.
- Excludes any time spent waiting for a response or action from the customer, Dell's employees, contractors, or any third-party provider outside Dell's control.
- Measurement: number of tickets by priority category restored within the SLA target as a percentage of all tickets in that priority category for the calendar month.
- Upon escalation to other parties such as Microsoft, incidents follow Service Levels of the receiving party.



Internal Use - Confidential

## Additional Plan Details

**Scope.** Support Plans cover all Azure Services covered by this Service Description. This Service does not include hardware, software or networking issues covered by Dell ProSupport (http://www.dell.com/en-us/work/learn/by-service-typesupportservices).

**Term.** The minimum term for any paid Managed Services plan is 3 months (one quarter). Billing and payment is upfront.

**Offer Availability.** Support Plans are available in markets in which Azure Cloud Services from Dell are offered.

**Tier Changes.** You may change your Managed Services tier with written notice to your account manager, allowing time to adjust resource allocation.

**Cancellation Policy.** Paid Managed Services plans require a commitment for the selected term. Cancellation will not result in a pro-rated refund.

**Upgrades.** Managed Services plans can be upgraded at any time by speaking with your Dell Azure account manager. Upgrades will be effective for a new term beginning on the purchase date of the upgraded service.

**Partner Commitment Period.** By subscribing to any paid Managed Services plan (Advanced, Premium, or Enterprise), you agree to maintain Dell as your primary Azure services provider for a minimum period of 365 days from the start date of your paid plan (the “Partner Commitment Period”), regardless of the commitment length selected for your Managed Services plan (3, 6, or 12 months).

This Partner Commitment Period reflects the significant investment Dell has made upon onboarding a paid Managed Services customer, including but not limited to: architecture and governance baselining, monitoring integration, compliance configuration, Surveil platform provisioning, cost optimization analysis, and ongoing managed services delivery.

**Partner Transfer Fee.** If, during the Partner Commitment Period, you elect to discontinue purchasing Azure Services through Dell — whether by transitioning to another provider, entering into a direct relationship with Microsoft, or through any other arrangement that results in Dell no longer serving as your Azure services provider — a Partner Transfer Fee will apply, calculated as follows:

**Partner Transfer Fee = 20% × (Monthly Average Azure Consumption Revenue × Remaining Months in Partner Commitment Period)**

Where:

- Monthly Average Azure Consumption Revenue is calculated as the average of your monthly Azure consumption over the 3 months immediately preceding the date of departure notification (or the full tenure if less than 3 months have elapsed).
- Remaining Months is the number of full or partial calendar months remaining between the date of departure notification and the end of the 365-day Partner Commitment Period.



Internal Use - Confidential

**Example:** A customer subscribes to the Premium plan on January 1, 2026. Their monthly average Azure consumption is $50,000. On November 1, 2026 (month 10 of 12), the customer notifies Dell of intent to depart. Two months remain in the Partner Commitment Period. The Partner Transfer Fee is calculated as: 20% × ($50,000 × 2) = $20,000.

The parties acknowledge that the Partner Transfer Fee represents a genuine pre-estimate of Dell's losses and costs arising from early departure, including but not limited to onboarding and integration costs, architecture baselining, monitoring configuration, Surveil provisioning, stranded service delivery capacity, and foregone margin. The Partner Transfer Fee is not intended as a penalty.

The Partner Transfer Fee will be invoiced upon notification of departure and is due prior to Dell's acceptance of any subscription transfer request in Microsoft Partner Center. Dell reserves the right to withhold subscription transfer processing until the Partner Transfer Fee is settled; provided, however, that any such withhold shall not extend beyond the ninety (90) day data migration period set forth in the Dell CSP Microsoft Usage Based Subscription Terms. If the Partner Transfer Fee remains unpaid at the expiration of the 90-day migration period, the outstanding amount shall constitute a debt obligation payable by you to Dell and may be pursued through Dell's standard collections process. You acknowledge that Dell requires access to billing and consumption data to calculate the Partner Transfer Fee, and you agree to cooperate in providing any data reasonably required for this calculation if transfer processing has occurred prior to fee settlement.

The Partner Transfer Fee is exclusive of any applicable taxes, levies, duties, or government-imposed charges, which shall be governed by the tax provisions of the applicable Commercial Terms of Sale.

The parties further acknowledge that Dell's losses from early departure include, but are not limited to, the loss of Microsoft program benefits allocated on an annualized basis, amortized onboarding and integration costs that are front-loaded in the first 30 days of service delivery, and stranded service delivery capacity that cannot be immediately reallocated. The parties agree that such losses would be difficult to calculate precisely at the time of contracting, and that the Partner Transfer Fee formula represents a reasonable methodology for approximating them.

For the avoidance of doubt:

- The Partner Commitment Period (365 days) is independent of and runs concurrently with the Managed Services commitment term (3, 6, or 12 months). Expiration of a Managed Services commitment term does not release you from the Partner Commitment Period if 365 days have not yet elapsed.
- Customers on the Standard plan (included at no additional cost) are not subject to the Partner Commitment Period or Partner Transfer Fee.
- If your paid Managed Services plan is not renewed after the initial commitment term but you remain a Dell CSP customer, the Partner Commitment Period continues until the 365-day anniversary of the original paid plan start date. During any period between the expiry of a paid Managed Services plan and the end of the Partner Commitment Period, Dell will continue to provide Standard plan services, Azure CSP billing, provisioning, and Surveil platform access as described in this Service Description.
- If the Partner Commitment Period has fully elapsed (365 days or more since the paid plan start date), no Partner Transfer Fee applies regardless of whether a paid Managed Services plan is still active.



Internal Use - Confidential

- The Partner Transfer Fee does not apply where (a) you genuinely discontinue all Azure consumption (reducing Azure Consumption Revenue to zero) without transferring workloads to another CSP partner, Microsoft direct agreement, or MACC arrangement; (b) your Azure subscription is terminated by Microsoft pursuant to the Microsoft Customer Agreement; or (c) the departure results from a force majeure event beyond your reasonable control.

## Hours of Service

Support is delivered remotely. All support services are available between 8AM to 5PM, Monday to Friday US Central Standard Time, except for 24/7 Break/Fix Support and Priority Escalation (Enterprise tier) which are available 24/7/365. Support is provided in English only.

## Support Channels

The following channels are available:

- Telephone — Inbound and Outbound (when needed). For P1/P2 incidents, customers must call in for fastest response.
- Email — Inbound and Outbound. Non-critical requests should be submitted via email.

## Quality Standards

The Services will align with good industry practice and the relevant manufacturer's recommendations and guidelines unless exempted by Dell via an acknowledged operational risk.



Internal Use - Confidential