Azure Management Services

Service Schedule

June 2026 Edition

Effective from 15 June 2026

Lanmark Limited
Company number 02977539
Registered office: West Hill House, West Hill, Dartford, DA1 2EU
lanmark.com/terms-of-business

Part of the Lanmark Terms of Business suite, published 15 June 2026.

Document control

Field	Value
Document title	Lanmark Limited Azure Management Services Schedule
Document reference	Lanmark Service Schedule: Azure Management
Version	June 2026 Edition
Document date	Effective from 15 June 2026
Status	Published (June 2026 Edition)
Supersedes	Nothing. New Service Schedule.
Layer	Layer 2 (Service Schedule) of the Lanmark T&C suite
Sits under	Lanmark Master Services Agreement (as in effect from time to time, published at lanmark.com/terms-of-business)

Revision history

Date	Version	Reason
15 June 2026	June 2026 Edition	First publication of the Lanmark Terms of Business suite (June 2026 Edition).

1. Purpose and scope

1.1 This Service Schedule sets out the service-specific terms on which Lanmark provides Azure Management Services to the Client. It supplements, and is to be read with, the Lanmark Master Services Agreement (MSA) and the Order Form.

1.2 Azure Management Services comprise Lanmark's management of the Client's Microsoft Azure environment, including (without limitation, and to the extent identified in the Order Form) continuous monitoring and operational oversight, patch and update management, Microsoft Defender for Cloud posture review and triage, Azure platform deprecation and change management, Azure-native backup oversight, incident response and remediation, advisory and architecture guidance, configuration assistance, operating-system support for Azure workloads, AVD and Azure-side access administration, Azure platform-tooling-based compliance support, and engagement management, in each case as further described at Clause 3. The Order Form identifies the Tier and the specific scope, hours allocation and Service Levels applicable to the engagement.

1.3 Azure Management Services are sold in one of two commercial shapes, identified in the Order Form:

(a) Hours Pack (Clause 3.6): a pre-purchased block of Azure engineer hours that the Client uses on demand for in-scope Azure management activity, sold per pack (typically per quarter or per year), with the Pack Hours and the Pack period stated in the Order Form;

(b) Monthly Managed Service (Clause 3.7): a recurring monthly managed Service per Azure tenancy, comprising the BAU managed activity included at the Tier identified in the Order Form, plus (where the Tier includes them) a monthly allowance of Reactive Hours for change, restore and operational remediation work.

1.4 Azure licensing and consumption itself is not within scope of this Schedule and is supplied under the Microsoft CSP Services Schedule. 24x7 Security Operations Centre (SOC) services, Security Information and Event Management (SIEM) and Managed Detection and Response (MDR) services are not within scope of this Schedule and are supplied under the Managed Cyber Security Services Schedule. Backup of Windows or Linux servers (whether in Azure or otherwise) and Microsoft 365 backup are supplied under the Backup Services Schedule. Wider IT support for the Client's broader environment outside the Azure estate is supplied under the IT Support Services Schedule. Co-location, IaaS and Application Hosting outside Azure are supplied under the Hosting Services Schedule. One-off Azure transformation, migration, modernisation and other project engagements are supplied under the Project Services Schedule.

1.5 Azure Management Services are a higher-risk Service because the Azure estate is typically business-critical and changes to it have direct operational consequences. This Schedule is to be read with that in mind, including the Service-specific disclaimers at Clause 9 and the Client indemnity at Clause 8.

1.6 Subject to Clause 1.3 of the MSA (order of precedence), this Schedule prevails over the MSA only in respect of the specific Service detail it covers and only where this Schedule explicitly states an override.

2. Definitions

The following definitions apply in this Schedule. Defined terms in the MSA have the meanings given to them in the MSA and are not redefined here.

Authorised User means an individual employee, contractor or representative of the Client whose use of the Client's Azure environment is administered as part of the Service.

BAU Managed Activity means the standing managed-service activity comprised in a Monthly Managed Service engagement, as described at Clause 3.7 and as further configured by Tier in the Order Form.

Business Day means any day other than a Saturday, Sunday or English bank holiday.

Hours Pack means a pre-purchased block of Azure engineer Pack Hours sold under the Hours Pack commercial shape described at Clause 3.6.

Microsoft means Microsoft Corporation and its affiliates, including Microsoft Limited (the UK Microsoft entity), as the provider of Azure, Microsoft Defender for Cloud, Microsoft Advanced Partner Support and the other Microsoft products and services that the Service supports or interacts with.

Microsoft Advanced Partner Support means the Microsoft Advanced Partner Support programme through which Lanmark, as a Microsoft Cloud Solution Provider, escalates Microsoft cloud incidents to Microsoft for problem resolution support, in accordance with Microsoft's published severity definitions and response times.

Monthly Managed Service means the recurring monthly managed Service shape described at Clause 3.7 and configured by Tier in the Order Form.

Pack Hours means the number of Azure engineer hours included in an Hours Pack, identified in the Order Form.

Pack Period means the period over which the Pack Hours are made available to the Client (typically per quarter or per year), identified in the Order Form.

Reactive Hours means the monthly allowance of Azure engineer hours included in a Monthly Managed Service Tier (where the Tier includes them) for reactive support, minor changes, restore operations and operational remediation activity, identified in the Order Form.

Service means in this Schedule, the Azure Management Services described in this Schedule (the Hours Pack shape, the Monthly Managed Service shape, or both, as identified in the Order Form).

Support Hours means Monday to Friday, 8.30am to 5.30pm UK time, excluding English bank holidays. Support Hours reflect the working rota of Lanmark's tier 3 Azure engineers and apply to Lanmark engagement management for this Service. The Support Hours for this Service are different from the Support Hours that apply under the IT Support Services Schedule (which are 8.00am to 6.00pm).

Tier means the Tier of Monthly Managed Service identified in the Order Form, configuring the BAU Managed Activity, Reactive Hours allowance, Service Levels and any add-ons applicable to the engagement.

3. Service description

Clauses 3.1 to 3.5 describe the substantive Azure management activity that may be included in either commercial shape. Clauses 3.6 and 3.7 describe the two commercial shapes (Hours Pack and Monthly Managed Service). The Order Form identifies which substantive activity is in scope, which commercial shape applies, and (for Monthly Managed Service) the Tier.

3.1 Monitoring and operational oversight

3.1.1 Continuous monitoring of in-scope Azure services and key health indicators, including availability, service performance, configured health alerts and key resource metrics. For clarity, continuous monitoring means that Lanmark's monitoring tooling runs continuously; Lanmark engineer triage, investigation, remediation and engagement management are performed during Support Hours unless the Order Form expressly provides for extended-hours or 24x7 cover.

3.1.2 Alert triage and investigation to determine cause and recommended remediation, escalation and coordination with Microsoft Advanced Partner Support where appropriate, and (where in scope at the engagement's Tier or Pack Hours allocation) remediation activity.

3.2 Patch and update management

3.2.1 Patch and update management for in-scope Windows and Linux virtual machines and other in-scope Azure resources, performed within agreed maintenance windows. The maintenance window arrangement is identified in the Order Form. Where the Client repeatedly misses, refuses or defers a maintenance window, the deferral is Client-controlled delay under Clause 5.3.2 and may affect Lanmark's ability to meet Service Levels or to maintain the Defender for Cloud security posture; Lanmark is not liable for the consequence of that Client-controlled deferral.

3.2.2 Patch exception handling where patches must be deferred for application or operational reasons, with the rationale recorded in the Service Tooling.

3.2.3 Reboot coordination and sequencing for dependent services, where required.

3.3 Vulnerability and configuration posture (Microsoft Defender for Cloud)

3.3.1 Periodic review of vulnerability and configuration posture for the in-scope Azure estate, including review, triage and prioritisation of Microsoft Defender for Cloud recommendations and remediation planning, in each case limited to findings visible through Microsoft Defender for Cloud and Azure platform tooling.

3.3.2 Lightweight security advisory under Clause 3.3.1 is limited to review, triage, prioritisation and Azure-platform remediation planning based on Microsoft Defender for Cloud findings and Azure platform-tooling output. For the avoidance of doubt, this Clause 3.3 does not include 24x7 Security Operations Centre (SOC) services, Security Information and Event Management (SIEM), Managed Detection and Response (MDR), independent vulnerability assessment, penetration testing, threat hunting, endpoint MDR, SIEM correlation, security incident containment outside Azure-platform remediation, security assurance, or any of the other deeper security services covered by the Managed Cyber Security Services Schedule

or the Cyber Assessments Services Schedule. Where the Client requires those deeper services in respect of the Azure estate, the Client subscribes in parallel to the Managed Cyber Security Services Schedule and/or the Cyber Assessments Services Schedule.

3.4 Azure platform deprecation and change management

3.4.1 Ongoing review of Microsoft Azure advisory notices, deprecation announcements and platform changes relevant to the in-scope Azure services, and recommendations to maintain compatibility, security posture and service continuity.

3.4.2 Planning and implementation of recommended Azure platform changes, where in scope of the Tier's included activity, the engagement's Reactive Hours allocation or the Hours Pack allocation; otherwise by separately-quoted work or by Project Services Schedule engagement.

3.5 Backup oversight, incident response and operational support

3.5.1 Oversight of configured Azure-native backup job success and failure for in-scope workloads, investigation of repeated failures and corrective actions where appropriate. Azure-native backup oversight under this Clause 3.5.1 is available as part of Azure Management independently of whether the Client also subscribes to the Backup Services Schedule. Where the Client does subscribe to the Backup Services Schedule, the actual backup of in-scope servers, the backup methodology, restore assurance, BCP virtualisation and any deeper backup responsibility are governed by that Schedule. For the avoidance of doubt, this Clause 3.5.1 is limited to job status oversight of configured Azure-native backup; it does not include backup design, restore assurance, recovery testing, business continuity planning, the identification of clean restore points following malicious activity, or any other deeper backup-service responsibility, unless the Client subscribes separately to the Backup Services Schedule or expressly contracts those activities in the Order Form. Restore operations are covered as described at Clause 3.7.3 below.

3.5.2 Incident response and remediation for Azure operational issues, including coordination with Microsoft under Clause 12 where appropriate. Lanmark engages Microsoft Advanced Partner Support on the Client's behalf for incidents that the Client has authorised Lanmark to escalate.

3.5.3 Configuration assistance, operating-system support strictly tied to in-scope Azure workloads, Azure Virtual Desktop and Azure-side access administration, where in scope of the Tier or Hours Pack allocation.

3.6 Hours Pack (commercial shape A)

3.6.1 Under the Hours Pack commercial shape, the Client purchases a defined block of Azure engineer Pack Hours, identified in the Order Form, to be used over a defined Pack Period (typically per quarter or per year, as identified in the Order Form).

3.6.2 Pack Hours are consumed against in-scope Azure management activity described at Clauses 3.1 to 3.5. The Client may direct Lanmark to use Pack Hours for any in-scope activity, with Lanmark's reasonable agreement on prioritisation and scheduling. Activity outside in-scope Azure management is not chargeable against Pack Hours. Pack Hours are consumed in

fifteen (15) minute increments unless the Order Form expressly states otherwise, consistent with Lanmark's standard IT Support pack billing increment.

3.6.3 Pack Hours that are not consumed within the Pack Period expire at the end of the Pack Period and are not refundable or carried forward, unless the Order Form expressly says otherwise.

3.6.4 Where the Client's demand exceeds the Pack Hours within the Pack Period, Lanmark may agree (at Lanmark's discretion) to provide additional engineer time on a time-and-materials basis, at Lanmark's then-current rate, or by Order Form variation to purchase an additional Pack.

3.7 Monthly Managed Service (commercial shape B)

3.7.1 Under the Monthly Managed Service commercial shape, the Client subscribes to a recurring monthly Service per Azure tenancy, at the Tier identified in the Order Form. The Tier identifies the BAU Managed Activity included and the Reactive Hours allowance (where the Tier includes one).

3.7.2 BAU Managed Activity is the standing scope of work Lanmark performs each month, comprising (subject to the Tier's specific configuration in the Order Form): the monitoring and operational oversight at Clause 3.1, the patch and update management at Clause 3.2, the vulnerability and configuration posture review at Clause 3.3, the platform deprecation and change management at Clause 3.4, the backup oversight at Clause 3.5.1, and the reporting and service review activity at Clause 6.6. BAU Managed Activity for reactive work, restore operations, configuration changes, AVD or access administration and minor remediation is performed against the Reactive Hours allocation (where the Tier includes one) or, where the engagement is at a Tier without a Reactive Hours allocation, by separately-quoted T&M work or by Hours Pack.

3.7.3 Reactive Hours allocations are calculated per billing month (aligned with the Monthly Managed Service billing period stated in the Order Form) and are not carried forward into the next billing month unless the Order Form expressly says otherwise. Where the Client's demand exceeds the Reactive Hours in a particular billing month, Lanmark may agree (at Lanmark's discretion) to provide additional engineer time on a time-and-materials basis at Lanmark's then-current rate, or to draw down against any Hours Pack the Client also holds.

3.7.4 Where the Client holds both a Monthly Managed Service engagement with a Reactive Hours allowance and an Hours Pack, reactive Azure management work is consumed in the following default order, unless the Order Form expressly says otherwise: (a) first, against the Reactive Hours allocation for the relevant billing month; (b) second, where the Reactive Hours are exhausted and the parties agree, against the available Hours Pack; (c) third, on a time-and-materials basis at Lanmark's then-current rate where neither Reactive Hours nor Hours Pack are available.

3.7.5 In plain terms, BAU Managed Activity covers the standing monthly Azure management tasks (monitoring, patching, posture review, deprecation tracking, backup oversight, reporting); Reactive Hours cover variable reactive work, minor changes, restore operations, AVD or access administration and incident remediation requested by the Client during the month. This Clause 3.7.5 is intended as a plain-English summary of Clauses 3.7.2 to 3.7.4 and is

operative for that purpose; where it conflicts with Clauses 3.7.2 to 3.7.4, those clauses prevail.

3.8 Compliance support (platform-tooling level)

3.8.1 Where the Order Form identifies it as in scope (and only to that extent), the Service includes compliance support at the level of Microsoft Defender for Cloud findings, Microsoft Compliance Manager output (where available), system-generated evidence and platform reporting. Compliance support of that kind comprises identification of compliance gaps visible via Microsoft platform tooling, support for the Client in completing compliance questionnaires using system evidence and Azure reporting, and recommended remediation actions.

3.8.2 Out of scope of this Clause 3.8 (unless separately contracted by Order Form variation, by Project Services Schedule engagement or by separately-quoted T&M work):

(a) manual audit-style assessment against the full text of any compliance control framework (such as SWIFT CSP, ISO 27001, Cyber Essentials Plus, NHS DSPT, FCA controls or equivalent);

(b) evidence pack production, control-by-control attestation activity, formal compliance certification, assurance reporting, audit sign-off responsibilities or interaction with an external auditor;

(c) ongoing compliance assurance, regular evidence refresh outside Lanmark's normal reporting cadence, or formal documented assurance outputs of any kind.

The Order Form may identify a deeper compliance support arrangement (for example, periodic SWIFT CSP documentation alignment review or an ongoing compliance retainer) as a separate add-on at separate Fees, in which case that arrangement is governed by the Order Form rather than this Clause 3.8. Any such Order Form arrangement may extend the in-scope activity within the platform-tooling perimeter of this Clause 3.8 (for example, broader questionnaire support, broader gap-review work, additional periodic documentation alignment) but does not, of itself, override the express exclusions at Clauses 3.8.2(a) to (c) or extend the Service into formal compliance certification, audit-style assurance, attestation activity or compliance assurance reporting. Where the Client requires formal certification, attestation or assurance, those services are supplied (where Lanmark is able to provide them) under the Cyber Compliance and Training Services Schedule, the Cyber Assessments Services Schedule or a Project Services Schedule engagement, as appropriate.

4. In scope and out of scope

4.1 In scope

The Service includes:

(a) the substantive Azure management activity at Clauses 3.1 to 3.5, to the extent identified in the Order Form;

(b) either the Hours Pack shape (Clause 3.6) or the Monthly Managed Service shape at the Tier identified in the Order Form (Clause 3.7), or both;

(c) the lightweight Defender for Cloud security layer at Clause 3.3.2;

(d) the platform-tooling-level compliance support at Clause 3.8, where the Order Form identifies it as in scope;

(e) Microsoft Advanced Partner Support pass-through under Clause 12;

(f) Lanmark engagement management during Support Hours;

(g) the Service Levels at Clause 5.

4.2 Out of scope

The following are out of scope of the Service and are not provided as part of the Service Fees. Where any of the following is required, it is provided (where Lanmark is able to provide it) as separately-quoted work or under a separate Service Schedule:

(a) Azure licensing and consumption (supplied under the Microsoft CSP Services Schedule);

(b) 24x7 Security Operations Centre (SOC) services, Security Information and Event Management (SIEM), Managed Detection and Response (MDR), threat hunting, security incident response beyond Azure-platform remediation, and any deeper security service (supplied under the Managed Cyber Security Services Schedule);

(c) backup of in-scope servers, Microsoft 365 backup and any backup methodology (supplied under the Backup Services Schedule; this Schedule covers only Azure-native backup oversight at Clause 3.5.1);

(d) wider IT support for the Client's environment outside the Azure estate (supplied under the IT Support Services Schedule);

(e) Co-location, IaaS and Application Hosting outside Azure (supplied under the Hosting Services Schedule);

(f) Azure FinOps, cost optimisation, reserved instance and savings plan advisory, Azure cost management, Azure cost governance, Azure budget management and any cost-control activity. For the avoidance of doubt, Lanmark does not take responsibility under this Schedule for Azure consumption costs or for advising on Azure cost optimisation, even at a light advisory level. Where the Client requires Azure cost optimisation work, it is supplied (where Lanmark is able to provide it) by separately-quoted project work under the Project Services Schedule;

(g) one-off Azure transformation, migration, modernisation, design, architecture or build engagements (supplied under the Project Services Schedule). This Schedule covers steady-state managed-service activity, not project delivery. For clarity, BAU Managed Activity and Reactive Hours under this Schedule are for in-life management of an established Azure estate, including incremental change, ongoing posture upkeep, ongoing patching, ongoing platform deprecation response, ongoing reactive remediation and minor configuration change; they are not for the design, build, migration, modernisation, transformation or first-time deployment of new Azure workloads, environments, landing zones, identity architectures or material new capability, which are supplied under the Project Services Schedule by a separate engagement;

(h) deeper compliance work (manual audit, attestation, certification, evidence pack production), save where the Order Form expressly identifies a deeper compliance arrangement under Clause 3.8 within the platform-tooling perimeter described there;

(i) Lanmark engineer attendance outside Support Hours, unless the Order Form expressly provides for extended hours or 24x7 engagement;

(j) anything stated as out of scope in the Order Form.

5. Service Levels

5.1 Priority taxonomy

5.1.1 Lanmark uses the following ITIL-style priority taxonomy for service requests and incidents in respect of the Azure estate:

Priority	Description
P1	Global or major Azure system failure affecting all Authorised Users, or critical business impact to the Client's operations
P2	Azure system failure affecting a significant subset or department of Authorised Users
P3	Support issue affecting fewer than five Authorised Users, or a non-critical operational issue
P4	Change Request, configuration change or planned work request
P5	Planned work, software updates, software requests or low-urgency requests

5.1.2 Priority is set on receipt of the request, automatically by the Service Tooling or by Lanmark engineers, in consultation with the Client where appropriate. Lanmark's priority classification, as recorded in the Service Tooling, is authoritative save in the case of manifest error. Priority may be reassessed during the lifetime of an incident if business impact changes.

5.2 Lanmark engagement response targets

5.2.1 Lanmark targets the following helpdesk response and escalation thresholds for Azure Management Service requests, measured during Support Hours from the time the request is received through the Service Tooling. The targets apply during Support Hours only; they do not create an obligation to respond outside Support Hours unless the Order Form expressly provides for extended-hours or 24x7 cover, in which case the Order Form sets out the out-of-hours arrangements and the applicable Fees. The targets are targets, not guarantees, and operate alongside the Microsoft Advanced Partner Support response times set out at Clause 12.2:

Priority	Helpdesk response	Escalation threshold
P1	0.5 hour	0.5 hour
P2	0.5 hour	1 hour
P3	1 hour	8 hours
P4	8 hours	16 hours
P5	48 hours	24 hours

5.2.2 Where the Order Form configures the engagement at a higher Tier with extended hours, faster response targets or 24x7 cover, those Tier-specific arrangements override the table at

Clause 5.2.1 for the relevant Priority and request type, as set out in the Order Form. The same difference in helpdesk response target between P1 and P2 (both 0.5 hour) reflects the urgency of triage; in practice the substantive escalation handling differs by Priority and Microsoft severity (Clause 12.2) once the ticket is open.

5.2.3 The Azure Management Service is a cloud-delivered Service and on-site response is not included in the standard table at Clause 5.2.1. On-site attendance is provided only where the Order Form expressly identifies it as part of the engagement, or where Lanmark and the Client agree in writing that on-site attendance is required for a particular incident. Where on-site attendance is in scope, the timing and Fees are set out in the Order Form or in the relevant written agreement.

5.3 Service Level measurement and exclusions

5.3.1 Lanmark's records held in the Service Tooling, the Azure activity logs and Lanmark's management systems are the authoritative record of Service Level performance, save in the case of manifest error.

5.3.2 Time spent waiting for Client action (including delay in providing access, approval, information or instructions, delay in nominating an Azure contact, or any other Client-controlled matter) does not count towards any applicable Service Level. Time spent in Microsoft's hands while Lanmark waits for Microsoft Advanced Partner Support engagement also does not count towards any applicable Lanmark Service Level (the Microsoft response times at Clause 12.2 apply separately to that activity).

5.3.3 The Service Levels at this Clause 5 are service management targets. They do not give rise to service credits, fee reductions, repayment of Fees or any similar monetary remedy. Where Lanmark fails to meet a Service Level target, Lanmark will use reasonable endeavours to investigate the cause and to remediate the underlying issue so that it does not recur. The Client's remedy is service review and escalation through the IT Support Services Schedule (where the Client subscribes to it in parallel) or through Lanmark's commercial contact for the engagement. Subject to Clause 18 of the MSA, this Clause 5.3.3 states the Client's full and exclusive remedy, and Lanmark's only obligation and liability, for non-performance or non-availability of the Service Levels at this Clause 5.

6. Operational arrangements

6.1 Onboarding

6.1.1 Onboarding includes the discovery of the in-scope Azure estate, agreement of the maintenance windows, configuration of the Lanmark Service Tooling against the Azure tenancy, configuration of monitoring alerts and access, agreement of the Authorised User and Azure-contact arrangements and initial baseline of the Microsoft Defender for Cloud posture. The expected duration of onboarding is identified in the Order Form.

6.1.2 Where the Client has agreed an onboarding Fee or technical onboarding manager fee, the Fee is identified in the Order Form.

6.2 Access to the Azure tenancy

6.2.1 The Service requires Lanmark to have administrative access to the Client's Azure tenancy and any associated Microsoft Entra (or equivalent identity provider) and Microsoft 365 tenancy, to the extent required to perform the in-scope activity. The Client will grant and maintain the required access, in accordance with the granular delegated admin privilege (GDAP) or equivalent access model in force from time to time.

6.2.2 Where Client-controlled access matters delay Lanmark's ability to perform the Service, time lost is Client-controlled delay under Clause 5.3.2 and the targets at Clause 5.2 do not run during that time.

6.3 Patch and change management

6.3.1 Patch management is performed within the agreed maintenance windows. The Client will cooperate with reboot coordination and dependent-service sequencing.

6.3.2 Material changes to the in-scope Azure estate proposed by Lanmark (for example, in response to an Azure deprecation, an architecture issue or a Defender for Cloud finding) are recommended to the Client and implemented either against the Reactive Hours allocation, the Hours Pack allocation, or by Order Form variation or separately-quoted T&M work, as appropriate. The Client's authorisation is required for material changes.

6.4 Reactive and remediation work

6.4.1 Reactive support, minor changes, restore operations, AVD and Azure-side access administration, incident remediation and similar reactive work is performed against the Reactive Hours allocation (where the engagement's Tier includes one), the Hours Pack allocation (where the engagement uses the Hours Pack shape), or (where neither covers the work) on time-and-materials terms agreed with the Client in writing.

6.4.2 Where the Client's reactive demand materially exceeds the available Reactive Hours or Pack Hours in a period, Lanmark will notify the Client and the parties will agree how the work is to be accommodated (additional Hours Pack purchase, Order Form variation to a higher Tier, time-and-materials terms, or deferral). Lanmark is not obliged to perform reactive work for which there is no available allocation and no agreed alternative commercial arrangement.

6.5 Microsoft Advanced Partner Support engagement

6.5.1 Where an Azure issue falls within the scope of Microsoft Advanced Partner Support, Lanmark engages Microsoft on the Client's behalf using Lanmark's CSP relationship and Microsoft severity assignment (Clause 12.2). Microsoft response times apply to Microsoft's engagement, not to Lanmark's engagement; the two operate alongside each other.

6.5.2 The Client is responsible for outlining the business impact of an incident so that Lanmark and Microsoft can agree the appropriate Microsoft severity (A, B or C). The Client may request a change of Microsoft severity during the lifetime of an incident where the business impact changes. Where the Client does not provide sufficient business-impact information when Lanmark requests it, Lanmark is not liable for any delay in Microsoft escalation, any lower severity allocation by Microsoft, or any Microsoft rejection of a requested severity classification that arises from the absence of that information.

6.6 Reporting and service review

6.6.1 For Monthly Managed Service engagements, Lanmark provides the Client with periodic Azure service reporting through the Service Tooling, including monitoring status, patching status, Defender for Cloud posture, incidents, change activity and key remediation actions. The standard reporting cadence is monthly. Reporting under this Clause 6.6.1 excludes Azure cost optimisation, cost governance and FinOps reporting unless the Order Form expressly includes them (consistent with Clause 4.2(f)). Where the Tier includes a service review meeting (recommended for higher-Tier engagements, including SWIFT, regulated or production-critical workloads), the service review meeting cadence is identified in the Order Form.

6.6.2 For Hours Pack engagements, Lanmark provides periodic reporting on Pack Hours consumption and the activity those hours have funded, at the cadence identified in the Order Form.

6.7 Support channels and hours

6.7.1 The Service is accessed through Lanmark's designated support channels (the Service Tooling, the published service desk email address and the published service desk telephone number).

6.7.2 Lanmark Azure engagement management is provided during Support Hours (Monday to Friday, 8.30am to 5.30pm UK time, excluding English bank holidays). Where the Order Form expressly provides for extended hours or 24x7 cover, the additional hours arrangement is as set out in the Order Form. The Microsoft Advanced Partner Support response window operates on Microsoft's published hours, which differ from Lanmark Support Hours.

7. Client responsibilities

To enable Lanmark to deliver the Service, the Client will:

(a) give Lanmark accurate information about the in-scope Azure estate, the existing arrangements, any third-party dependencies and any compliance, regulatory or sector-specific constraints that affect the engagement;

(b) grant and maintain Lanmark's administrative access to the Azure tenancy (and any associated Microsoft Entra and Microsoft 365 tenancy), under the granular delegated admin privilege (GDAP) or equivalent access model, and respond promptly to Lanmark consent requests where the access model requires Client approval for elevation;

(c) agree maintenance windows for patch and update activity, and cooperate with reboot coordination and dependent-service sequencing;

(d) authorise material changes to the in-scope Azure estate that Lanmark recommends, including changes required to address Azure deprecations, architecture issues or Defender for Cloud findings. Where the Client refuses, declines or materially delays an authorisation in response to a Lanmark recommendation in respect of an Azure deprecation, compatibility, security or platform-continuity matter, Lanmark is not liable for any consequent impact, and the Client takes the residual risk of that decision;

(e) notify Lanmark of any move, change, retirement or addition of in-scope Azure resources (for example, the deployment of new servers, the retirement of a workload, the migration of a workload to or from Azure, or the change of an Azure subscription) so that scope and Fees can be adjusted by Order Form variation under the MSA, or through Reactive Hours, Hours Pack or separately-agreed T&M where Lanmark considers that appropriate to the size of the change;

(f) be responsible for the Client's own Azure consumption costs, Azure cost decisions, Azure budget setting and Azure cost optimisation decisions (which are out of scope of this Schedule under Clause 4.2(f));

(g) nominate an Azure contact at the Client to authorise Azure Management Service requests, accept change implementation, agree maintenance windows, agree Microsoft severity assignment and receive Service-related communications. Lanmark may rely on instructions, approvals, sign-offs and decisions from the nominated Azure contact unless the Client notifies Lanmark otherwise in writing;

(h) respond promptly to Lanmark requests for information, access, approval or instructions in connection with the Service;

(i) notify Lanmark before onboarding (and from time to time as relevant during the Service) where the Azure estate will routinely process substantial volumes of special category Personal Data, criminal offence data, children's data or other unusually sensitive data, where the nature of that data affects the configuration, regulatory classification, technical design or security posture of the Service (Clause 10);

(j) comply with the Microsoft Customer Agreement and any other Microsoft terms applicable to the Client's Azure tenancy, including any acceptable use, support, security or compliance terms that Microsoft publishes from time to time;

(k) where the Client requires deeper security services, deeper compliance services, backup of in-scope servers, wider IT support or one-off Azure project work, subscribe to the relevant Lanmark Service Schedule (Managed Cyber Security, Backup, IT Support, Project Services) or commission separately-quoted work to provide the required scope;

(l) where applicable, not provide individual Authorised User passwords, secrets or credentials to Lanmark unless Lanmark expressly requests them for a defined Service purpose and a secure process is used.

Where the Client does not meet a responsibility under this Clause 7, and that failure causes or materially contributes to a Service failure, a delay in delivery, a Client loss arising in connection with the Service or a third-party claim, Lanmark is not liable for the consequent loss or damage, and the Client's indemnity at Clause 8 applies to the extent set out in Clause 8.

8. Indemnification

8.1 The Client will indemnify Lanmark against any third-party claim made against Lanmark (including regulatory action by any regulator or supervisory authority, and including claims by employees, customers or counterparties of the Client), and against Lanmark's reasonable costs and expenses (including reasonable legal fees) incurred in connection with such third-party claim or regulatory action, in each case to the extent the claim or action arises out of or in connection with:

(a) the Client's breach of any obligation under this Schedule, the MSA, the Microsoft Customer Agreement or any Microsoft terms applicable to the Client's Azure tenancy, where those Microsoft terms have been made available to the Client or are generally published by Microsoft;

(b) the Client's failure to provide accurate or complete information about the Azure estate or to notify a material change as required under Clause 7(e);

(c) any data, content, workload or configuration that the Client (or any party acting under the Client's instruction or control) provides, places in or on the Azure tenancy, or instructs Lanmark to migrate, configure, expose, publish, connect, secure or use as part of the Service, where the data, content, workload or configuration is unlawful, infringes a third-party right or breaches an applicable law, regulation, code of conduct or acceptable use rule, save to the extent that the relevant act is at Lanmark's instruction or is caused by Lanmark's unauthorised modification or misuse;

(d) the Client's Azure consumption costs, Azure cost decisions, Azure budget overruns, Azure cost optimisation decisions or any consumption-based Microsoft charge (which are out of scope of this Schedule under Clauses 4.2(f) and 7(f)), where such matter gives rise to a third-party claim or regulatory action against Lanmark, and except to the extent caused by Lanmark's gross negligence, wilful misconduct, breach of a non-excludable obligation under the MSA or applicable law, or Lanmark's unauthorised use or unauthorised configuration of the Client's Azure tenancy. For the avoidance of doubt, Lanmark's first-party right to be paid for Azure consumption is dealt with at Clause 13.6, not under this indemnity;

(e) the Client's failure to subscribe to deeper security services (under the Managed Cyber Security Services Schedule) or to maintain backup arrangements (under the Backup Services Schedule), where Lanmark has recommended those services in writing (whether in the Order Form, in a service review, in a written risk note or otherwise in writing), the Client has elected not to proceed, and the failure causes or materially contributes to the third-party claim;

(f) any third-party claim arising from compliance certification, attestation or audit-style assurance representations that the Client (or any party acting under the Client's instruction or control) makes beyond the platform-tooling evidence and the specific written wording that Lanmark has expressly approved in writing for that representation.

8.2 The indemnity at Clause 8.1 does not apply to the extent that the matter giving rise to the third-party claim or regulatory action is caused by the gross negligence or wilful misconduct of Lanmark, or by Lanmark's breach of a non-excludable obligation under the Data Protection

Legislation, the MSA or applicable law. For the avoidance of doubt, the indemnity is given without prejudice to, and does not narrow, the non-excludable carve-outs at Clause 18.1 of the MSA.

8.3 The Client's indemnity at this Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA (including the per-Service per-Contract Year cap at Clause 18.2 and the exclusions at Clause 18.3 of the MSA). Clause 18.2.2 of the MSA applies.

8.4 Lanmark will give the Client prompt written notice of any third-party claim or regulatory action that may give rise to an indemnity under Clause 8.1, and will not settle or admit liability without the Client's prior written consent (such consent not to be unreasonably withheld or delayed). The Client may take conduct of the defence at the Client's cost where Lanmark gives its prior written approval, such approval not to be unreasonably withheld. Lanmark may refuse approval where, in Lanmark's reasonable opinion, the claim or regulatory action concerns Lanmark's own legal, regulatory, confidentiality or reputational interests, including (without limitation) any matter involving Lanmark's confidential information, Lanmark's Microsoft CSP relationship, Lanmark's tooling and methodology, other clients of Lanmark, or any direct investigation of Lanmark by a regulator or other authority. Where Lanmark refuses approval, Lanmark will assume conduct of the defence and will keep the Client reasonably informed.

9. Disclaimers

9.1 Azure Management Services depend on the operation of the Microsoft Azure platform, Microsoft Advanced Partner Support, Microsoft Defender for Cloud and other Microsoft products and services. The Service does not guarantee uninterrupted Azure operation or any particular Azure outcome in every circumstance. In particular, and without limitation, Lanmark does not warrant or guarantee that:

(a) Microsoft Azure, Microsoft Defender for Cloud or any other Microsoft product or service will operate without interruption, fault, downtime or vulnerability;

(b) any monitoring, patching, vulnerability review, posture remediation or other in-scope activity will prevent every Azure incident, security event, deprecation impact or service degradation;

(c) the Microsoft Advanced Partner Support engagement will resolve any particular incident within the Microsoft published response time, or at all, where that resolution depends on Microsoft's own operational and engineering capacity;

(d) data deleted, modified or encrypted by malicious activity (including ransomware) will be recoverable where the affected data is also affected on the backup or restore point before a clean restore point is available. For the avoidance of doubt, Azure Management Services are not security or threat-detection services (those services sit under the Managed Cyber Security Services Schedule), are not backup services (those services sit under the Backup Services Schedule), and do not include the identification of clean restore points, backup assurance or threat detection in respect of the in-scope Azure estate unless the Order Form expressly says otherwise. The lightweight Defender for Cloud layer at Clause 3.3 does not give rise to a Lanmark duty to detect malicious activity;

(e) the platform-tooling compliance support at Clause 3.8 will identify every compliance gap or constitute (or be a substitute for) a formal compliance certification, attestation or audit-style assurance.

9.2 Microsoft products and services are supplied to the Client under the Microsoft Customer Agreement and other Microsoft terms applicable to the Client's tenancy. Lanmark does not give any separate warranties (express, implied or statutory) in respect of any Microsoft product or service, save to the extent that any such warranty cannot be excluded under applicable law. This Clause 9.2 does not exclude any warranty or other obligation that cannot be excluded under applicable law, and does not affect Lanmark's own obligation to deliver the Service in accordance with the MSA and this Schedule.

9.3 Subject to Clause 18 of the MSA, Lanmark is not liable for any Service failure, Azure outage, security incident, compliance gap, cost overrun, loss of data or interruption to the Client's business that is caused by Microsoft operating its products or services in accordance with the Microsoft Customer Agreement and the other Microsoft terms, environmental conditions, human error of the Client, third-party action, or any other factor outside Lanmark's reasonable control, including (without limitation) Client-side configuration choices, Client or third-party changes to the Azure tenancy or to dependent systems, insufficient or expired Azure licences, the Client's failure to maintain backup or security arrangements (whether under another Lanmark Service Schedule or otherwise), Client resource availability changes, and

Client-controlled deferral of recommended deprecation, security or platform-continuity changes, except to the extent caused by Lanmark's breach of an express obligation under this Schedule or the MSA, the gross negligence or wilful misconduct of Lanmark, or Lanmark's breach of a non-excludable obligation under the Data Protection Legislation, the MSA or applicable law.

9.4 The Client acknowledges that Azure management is one element of a broader operational, security, compliance, backup and resilience posture. The Service is designed to support the Client's day-to-day Azure operation at the agreed Tier or Pack Hours level. It is not a substitute for the Client's own broader business continuity arrangements, security controls, backup arrangements, compliance assurance arrangements, cost governance or operational governance, and it does not transfer the Client's residual operational risk in those areas to Lanmark.

10. Data protection particulars

This Clause 10 supplements Clause 13 (Data protection) of the MSA and sets out the Article 28 processing particulars for the Service. Defined terms in Clause 13 of the MSA apply in this Clause. Azure Management Services involve Lanmark administering the Client's Azure tenancy under granular delegated admin privilege; Lanmark may incidentally access Personal Data on the tenancy in the course of monitoring, patching, posture review, change implementation and remediation.

Article 28 particular	Value for the Azure Management Service
Subject matter of the processing	Provision of the Azure Management Services, comprising Lanmark's administrative management of the Client's Azure tenancy, including monitoring, patch and update management, vulnerability and configuration posture review, Azure platform deprecation and change management, Azure-native backup oversight, incident response, advisory and (where in scope) platform-tooling compliance support.
Duration of the processing	For the duration of the Service. Lanmark-held records relating to Service operation (monitoring records, patch records, ticket records, change records, Defender for Cloud findings, incident notes, reporting and Microsoft Advanced Partner Support engagement records) are governed by Lanmark's Data Protection and Retention Policy. Temporary diagnostic extracts, exported logs, evidence files and working copies created by Lanmark during investigation, remediation or Microsoft escalation are deleted, returned or retained in accordance with the Client's written instructions, Lanmark's Data Protection and Retention Policy, the Order Form and applicable law. Microsoft-held records relating to the Azure tenancy itself are governed by the Microsoft Customer Agreement and Microsoft's published retention and data-handling positions.
Nature and purpose of the processing	Collection, organisation, storage, retrieval, use, transmission and (where applicable) deletion of Personal Data for the purpose of administering the Client's Azure tenancy and delivering the in-scope Azure management activity. Lanmark accesses Personal Data only to the extent necessary to perform the agreed Service.
Types of Personal Data	Personal Data of Authorised Users and Azure administrators (names, email addresses, account identifiers and identity provider attributes); Personal Data contained in workloads, configurations, logs or telemetry that Lanmark incidentally encounters when administering the Azure tenancy; and Personal Data contained in support ticket content, screenshots, diagnostic outputs, exported logs, Azure activity logs, Defender for Cloud recommendations, backup job metadata, Microsoft support case data, change records and Microsoft Advanced Partner Support engagement records produced or processed in the course of the Service. Lanmark does not select, filter or curate Personal Data within the Azure tenancy, except where strictly necessary to perform the Service or to give effect to a specific written Client instruction.
Categories of data subject	Authorised Users; Client employees, contractors and customers whose Personal Data is held in the in-scope Azure tenancy; and any other category of data subject identified in the Order Form.

Documented instructions for processing	Set out in the MSA, this Schedule, the Order Form, the Lanmark service documentation produced during onboarding, and any further written instructions the Client gives Lanmark from time to time. The Microsoft Customer Agreement informs the underlying Azure processing terms; the Client's instructions to Lanmark in respect of Lanmark's administrative activity remain governed by the MSA and the Data Protection Legislation.

For clarity, Lanmark's processing under this Schedule is limited to the administrative activity required to deliver the Service. Microsoft's processing of Azure tenancy data, including platform telemetry, Defender for Cloud findings, support data, Microsoft Advanced Partner Support engagement records and any data Microsoft processes pursuant to its statutory or regulatory obligations as a cloud-services provider, is governed by the Microsoft Customer Agreement and Microsoft's own data-protection commitments. Microsoft acts independently of Lanmark for that processing, and Lanmark does not warrant Microsoft's compliance with those commitments.

The Client authorises Lanmark to disclose relevant support, diagnostic, ticket, telemetry, configuration and escalation data to Microsoft where escalation to Microsoft Advanced Partner Support, or other Microsoft engagement reasonably required to deliver the Service, makes that disclosure necessary or appropriate. Microsoft's processing of any such disclosed data is governed by the Microsoft Customer Agreement and Microsoft's own data-protection commitments.

Where the Azure tenancy will routinely contain substantial volumes of special category Personal Data, criminal offence data, children's data or other unusually sensitive data, and where the nature of that data affects the configuration, regulatory classification, technical design or security posture of the Service, the Client will inform Lanmark before onboarding so that appropriate technical and organisational measures (and any Order Form scope adjustments) can be confirmed.

11. Sub-Processors used in delivering this Service

Lanmark uses Sub-Processors to deliver the Service in accordance with Clauses 13.5 to 13.7 of the MSA. Microsoft's role in this Service is set out separately below the Sub-Processor table, because Microsoft is the underlying Azure platform provider rather than (in the ordinary course) a Lanmark Sub-Processor. The categories of Lanmark Sub-Processor used in delivering this Service are:

Category	Role in this Service
Service Tooling and monitoring providers	Provision of the Lanmark service management, monitoring and ticketing systems used to administer the Azure engagement, including configuration of monitoring alerts, ticket records and reporting. Where the provider processes Personal Data on Lanmark's behalf in connection with the Service, the provider is a Sub-Processor.
Azure Management Tooling provider(s)	Where Lanmark uses a third-party Azure management, discovery, assessment, automation, remediation or reporting tool in the course of delivering the Service (in addition to standard Service Tooling), and that tool processes Personal Data on Lanmark's behalf in connection with the Service, the tool provider is a Sub-Processor.
Lanmark-engaged Sub-Contractors and specialist Azure consultants	Where Lanmark engages a third-party sub-contractor or specialist Azure consultant to perform any element of the Service, that sub-contractor or consultant is a Sub-Processor where it processes Personal Data on Lanmark's behalf in connection with the Service.

Microsoft (as defined in Clause 2) is the operator of the Microsoft Azure platform, Microsoft Defender for Cloud, the Microsoft Customer Agreement, Microsoft Advanced Partner Support, Microsoft Entra and the other Microsoft products and services that this Service supports or interacts with. Microsoft is not a Lanmark Sub-Processor for the underlying Azure tenancy; Microsoft acts independently of Lanmark for the Azure platform, and the Client has a direct relationship with Microsoft under the Microsoft Customer Agreement. Microsoft is a Sub-Processor for this Service only to the extent that Microsoft processes Personal Data on Lanmark's behalf in connection with the administrative engagement (for example, in CSP partner-side tooling where Lanmark expressly instructs Microsoft to perform an action on Lanmark's behalf, or in Microsoft Advanced Partner Support engagement records produced as a result of Lanmark's escalation). The Sub-Processors List identifies any such conditional Microsoft Sub-Processor arrangements that operate at any time.

The current Sub-Processor in each category is identified in the live Sub-Processors List published at lanmark.com/terms-of-business. The Sub-Processors List is the authoritative source for the identification of current Sub-Processors, the location of processing and any applicable international transfer mechanism.

12. Relationship with Microsoft

12.1 Microsoft is the supplier of the underlying Azure platform, Microsoft Defender for Cloud, Microsoft Advanced Partner Support and the other Microsoft products and services that this Service supports or interacts with. Lanmark is a Microsoft Cloud Solution Provider with access to Microsoft Advanced Partner Support, and, where applicable, engages Microsoft on the Client's behalf in connection with this Service. The substantive Azure platform is operated by Microsoft, not by Lanmark.

12.2 Microsoft Advanced Partner Support response times

12.2.1 Where a Microsoft cloud-services issue falls within scope of Microsoft Advanced Partner Support, Microsoft's published severity definitions and response times apply to Microsoft's engagement. The table below is illustrative only and reflects Microsoft's published severities and indicative response times as at the date of this Schedule. Microsoft may change those severities and response times from time to time, and the position published by Microsoft from time to time prevails over the table:

Microsoft severity	Description	Expected first-call response
Severity A	Critical business impact, significant loss or degradation of services (application down)	1 hour or less, with escalation management
Severity B	Moderate business impact; moderate loss or degradation of services, work can reasonably continue in an impaired manner	2 hours or less, available during business hours only
Severity C	Minimum business impact; substantially functioning with minor or no impediments to services	4 hours or less, available during business hours only

12.2.2 Microsoft severity definitions, response times and the applicable Microsoft business hours for Severity B and C engagement are as published by Microsoft from time to time, and are subject to change by Microsoft from time to time. The position published by Microsoft from time to time prevails over any indicative description in this Schedule.

12.2.3 Lanmark engages Microsoft Advanced Partner Support on the Client's behalf and uses reasonable endeavours to keep the Client informed of Microsoft's engagement on a Microsoft ticket. Lanmark does not commit to operating standards or response times for Microsoft Advanced Partner Support that are different from, or more onerous than, those published by Microsoft. Where Microsoft fails to meet a published response time, Lanmark's obligation and liability in respect of that failure is limited to using reasonable endeavours to escalate within Microsoft Advanced Partner Support and to keep the Client informed. This Clause 12.2 is a Service-specific application of Clauses 11.2, 17.4 and 18.4 of the MSA.

12.3 Microsoft platform changes

12.3.1 Microsoft Azure is a fast-moving platform. Microsoft may make changes to Azure services, features, pricing, supported product range, deprecation timelines and operating standards from time to time. Lanmark monitors Azure advisory and deprecation notices and recommends Client action where required (Clause 3.4). Microsoft-imposed changes may take effect on Microsoft's timetable (including immediately or mandatorily, for regulatory, security or operational reasons) and may apply before Lanmark is able to give advance notice to the Client. Lanmark will give the Client notice of such changes as soon as reasonably practicable after Lanmark receives notice from Microsoft.

12.3.2 Where the Service depends on the operation of the Microsoft Azure platform, Lanmark's obligations under this Schedule are subject to Microsoft operating the platform in accordance with the Microsoft Customer Agreement and the other Microsoft terms. Subject to Lanmark's obligations under Clause 13 of the MSA and the Data Protection Legislation in respect of any Sub-Processors, Lanmark is not liable for any act or omission of Microsoft, including any failure of the Azure platform to operate as expected, any change in the Microsoft Customer Agreement, any Microsoft-imposed end-of-life of a product, or any change in the Microsoft pricing or operating model.

13. Service-specific commercial terms

13.1 Fees and pricing

13.1.1 The Fees for the Service are set out in the Order Form. The Order Form identifies the commercial shape (Hours Pack or Monthly Managed Service), the Tier (for Monthly Managed Service), the Pack Hours and Pack Period (for Hours Pack), the Reactive Hours allowance (where the Tier includes one), the Fees for any add-on activity (for example, deeper compliance support under Clause 3.8) and the Fees for any separately-quoted work.

13.1.2 Time-and-materials work performed under Clause 6.4 outside the Reactive Hours or Pack Hours allocation is invoiced separately at Lanmark's then-current rate, and is payable at the time the work is performed.

13.1.3 The Fees referred to in this Clause 13.1 are reviewed by Lanmark from time to time and may be adjusted in accordance with the MSA fee-adjustment provisions (Clauses 7.9, 7.10 and 7.11). Microsoft rate or product changes that affect the Azure platform are not, of themselves, Lanmark Fee adjustments; Azure consumption costs are outside this Schedule under Clauses 4.2(f) and 7(f) in any event.

13.2 Term and renewal

13.2.1 Monthly Managed Service engagements are supplied on the Initial Term and Subsequent Term set out in the Order Form. The default non-renewal notice period is ninety (90) days before the end of the then-current Term, consistent with the MSA default at Clause 20.2.

13.2.2 Hours Pack engagements are supplied for the Pack Period stated in the Order Form. Where the Order Form provides for automatic renewal of an Hours Pack at the end of the Pack Period, the renewal arrangements and any non-renewal notice are as set out in the Order Form.

13.3 Termination charges

13.3.1 Where the Client terminates a Monthly Managed Service engagement before the end of the Initial Term or the then-current Subsequent Term, for any reason other than the Client's right to terminate for Lanmark's material breach under Clause 20 of the MSA, the Client remains liable for the Fees through to the end of that Term.

13.3.2 Where the Client terminates an Hours Pack engagement before the end of the Pack Period, the Client is not entitled to a refund of any Pack Hours that have not been consumed; Pack Hours not consumed in the Pack Period expire under Clause 3.6.3.

13.3.3 Clauses 13.3.1 and 13.3.2 reflect that Lanmark's delivery of the Service involves engineer capacity allocation and engagement management that Lanmark cannot recover on Client early termination.

13.3.4 The parties agree that the Client's payment obligation under this Clause 13.3 is a primary payment obligation reflecting the agreed commercial commitment for the Term or Pack Period, and is not a penalty or a secondary damages remedy. The parties have negotiated and accepted the Fees on this basis.

13.3.5 Clause 13.3 is a Service-specific application of Clause 20 of the MSA and prevails over any inconsistent position the MSA might otherwise be read to allow for this Service.

13.3.6 On termination of the Service for any reason, the Client remains liable to pay (in accordance with the MSA payment terms): all Fees accrued and unpaid up to the date of termination; any time-and-materials Fees, additional Pack purchase Fees, add-on Fees under Clause 3.8 and Fees for any other separately-quoted work performed up to the date of termination; any Reactive Hours used in excess of the Reactive Hours allocation for the relevant billing month; any Microsoft, third-party Sub-Processor or other pass-through costs that Lanmark has incurred on the Client's behalf in connection with the Service; and any other amount that has accrued under this Schedule or the MSA on or before the date of termination. Lanmark may invoice the Client for any such amounts after termination, whether the relevant activity took place before or after the date of termination, and the Client will pay each such invoice in accordance with the MSA payment terms.

13.4 Direct Debit and invoicing

13.4.1 The Client agrees to pay all invoices for the Service by Direct Debit, in accordance with the MSA Direct Debit position for recurring and consumption-based Services, save where the Order Form or the relevant invoice expressly identifies an alternative payment method (for example, BACS for one-off Hours Pack purchases, time-and-materials Fees or add-on Fees), in which case the alternative method applies to that Fee. Hours Pack purchase Fees, time-and-materials Fees and Fees for add-on activity under Clause 3.8 are invoiced separately at the time the relevant activity is performed or the relevant pack is purchased.

13.5 Suspension for non-payment

13.5.1 Where the Client fails to pay an invoice for the Service when due, Lanmark may (in addition to the rights and remedies in the MSA) suspend further Service activity until the overdue invoice is paid. Lanmark may, at Lanmark's discretion (and is not obliged to), continue safety-relevant or stability-relevant monitoring during the suspension period; any such monitoring is provided on a discretionary basis only and does not constitute a waiver of Lanmark's suspension rights. Where suspension affects in-scope BAU Managed Activity or Reactive Hours availability, the consequence is treated as Client-controlled delay under Clause 5.3.2, and Lanmark is not liable for any Service impact during the suspension period.

13.5.2 For the avoidance of doubt, Reactive Hours allocations for the affected billing month and Pack Hours in the affected Pack Period continue to expire in accordance with Clauses 3.7.3 and 3.6.3 during any period of suspension under Clause 13.5.1. Suspension does not extend the Pack Period, suspend the expiry of unused Reactive Hours or Pack Hours, or entitle the Client to a refund or credit in respect of them.

13.6 Client responsibility for Azure consumption and Microsoft charges

13.6.1 Azure consumption, usage, overrun, budget management, cost optimisation, fraud-related consumption and any consumption-based Microsoft charge arising through or in connection with the Client's Azure tenancy are out of scope of this Schedule under Clauses 4.2(a), 4.2(f) and 7(f), and are the Client's responsibility. Where Lanmark, in its capacity as Microsoft CSP under the Microsoft CSP Services Schedule, invoices the Client for Azure consumption or

other consumption-based Microsoft charges, the Client agrees to pay those invoices in accordance with the Microsoft CSP Services Schedule terms.

13.6.2 Without limitation, the Client is responsible for Azure consumption, usage and consumption-based Microsoft charges (and Lanmark is not liable for the cost of them) arising from: any deployment, scaling, configuration, automation or operating decision made by the Client or by any party acting under the Client's instruction or control; any Azure resource that the Client has authorised Lanmark to deploy, scale, modify or operate as part of the Service; any unauthorised use, account compromise, credential leak or fraudulent activity affecting the Client's Azure tenancy or its associated identity provider; any growth in Azure consumption or change in the Microsoft pricing or operating model from time to time; any cost spike, anomaly, runaway resource or unexpected charge that the Client has not configured Azure platform tooling to flag or cap; and any other consumption or charge that does not arise from Lanmark's gross negligence, wilful misconduct, breach of a non-excludable obligation under the MSA or applicable law, or Lanmark's unauthorised use or unauthorised configuration of the Client's Azure tenancy.

13.6.3 The Client's payment obligation under this Clause 13.6 is a primary payment obligation reflecting the underlying commercial position that the Client is the customer of record for its own Azure tenancy and bears its own Azure consumption cost. The Client may raise a genuine dispute about an Azure consumption invoice in accordance with the MSA payment dispute process and is not required to pay the genuinely disputed amount while that process is followed. However, the Client must pay all undisputed amounts on the due date, and may not refuse, withhold or set off payment of Azure consumption invoices on the basis of any dispute about Azure Management Services or any other Lanmark Service Schedule, except to the extent expressly permitted by the MSA payment terms.

14. Explicit overrides of the Master Services Agreement

Clause 1.3 of the MSA provides that a Service Schedule prevails over the MSA only in respect of specific service detail and only where the Service Schedule explicitly states an override. The following provisions of this Schedule are explicit overrides of the MSA for the Azure Management Service:

(a) Clause 5 of this Schedule sets the Service-specific Service Level position: ITIL P1 to P5 priority taxonomy with the response targets at Clause 5.2 (varying by Tier as the Order Form configures); the Azure Management Service is cloud-delivered and on-site response is not included in the standard table, with on-site attendance applying only where the Order Form expressly provides for it or where the parties agree in writing under Clause 5.2.3; Microsoft Advanced Partner Support response times at Clause 12.2 apply separately to Microsoft engagement and Microsoft engagement time does not count against Lanmark targets; Service Levels are targets not guarantees and do not give rise to service credits, with the Client's remedy being reasonable-endeavours investigation and remediation of the underlying service-management issue, where within Lanmark's control, as set out in Clause 5.3.3, and service review and commercial escalation. This is a Service-specific application of Clauses 17.4 and 18.4 of the MSA;

(b) Clause 8 of this Schedule sets out a Service-specific indemnity from the Client to Lanmark, limited to third-party claims and regulatory action against Lanmark, and to Lanmark's reasonable costs and expenses incurred in responding, in each case to the extent the claim or action arises from Client-controlled risk in this Service (including inaccurate information, breach of Microsoft terms, unlawful Azure workload content, Azure consumption decisions, failure to subscribe to deeper security or backup arrangements, and compliance representations made by the Client beyond Lanmark's platform-tooling compliance support). The indemnity at Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA, including the non-excludable carve-outs at Clause 18.1;

(c) Clause 9 of this Schedule sets out Service-specific disclaimers, including that Microsoft Azure, Microsoft Defender for Cloud and Microsoft Advanced Partner Support are not guaranteed to operate without fault or interruption, that the in-scope management activity will not prevent every Azure incident or security event, that platform-tooling compliance support is not a substitute for formal compliance certification, and that Lanmark is not liable for Service failure caused by factors outside Lanmark's reasonable control. Clause 9.3 preserves Lanmark's liability for its own breach of an express obligation under the Schedule or the MSA, gross negligence, wilful misconduct, and breach of non-excludable obligations;

(d) Clauses 1.4 and 4.2 of this Schedule set out the boundary with the rest of the suite: Azure licensing and consumption sit under the Microsoft CSP Services Schedule; 24x7 SOC, SIEM and MDR sit under the Managed Cyber Security Services Schedule; backup of in-scope servers and Microsoft 365 backup sit under the Backup Services Schedule; wider IT support sits under the IT Support Services Schedule; Co-location, IaaS and Application Hosting outside Azure sit under the Hosting Services Schedule; one-off Azure projects sit under the Project Services Schedule. Azure FinOps, Azure

cost optimisation, Azure cost management and Azure cost governance are not within scope of this Schedule under Clauses 4.2(f) and 7(f), regardless of any informal advisory exchanged in the course of engagement management;

(e) Clause 12 of this Schedule sets out the Microsoft Advanced Partner Support pass-through position: Microsoft severities A, B and C and Microsoft's published response times apply to Microsoft's engagement; Lanmark does not commit to Microsoft-side response times more onerous than Microsoft publishes; Lanmark's obligation and liability for Microsoft Advanced Partner Support failures is limited to reasonable endeavours to escalate within Microsoft and to keep the Client informed. This is a Service-specific application of Clauses 11.2, 17.4 and 18.4 of the MSA;

(f) Clause 13.3 of this Schedule sets out a Service-specific termination charges position: for Monthly Managed Service engagements, the Client remains liable for the Fees through to the end of the Term on any termination other than for Lanmark material breach; for Hours Pack engagements, unconsumed Pack Hours expire at the end of the Pack Period under Clause 3.6.3 and are not refundable on early termination. The termination charges are framed as a primary payment obligation. This is a Service-specific application of Clause 20 of the MSA;

(g) Support Hours for this Service at Clause 2 (Monday to Friday, 8.30am to 5.30pm UK time) differ from the Support Hours under the IT Support Services Schedule (8.00am to 6.00pm), reflecting the working rota of Lanmark's tier 3 Azure engineers.

Save as set out above, this Schedule does not override the MSA. Any provision of this Schedule that conflicts with the MSA without expressly stating an override under this Clause 14 is to be read consistently with the MSA in accordance with Clause 1.3 of the MSA.