SERVICE ORDER: Kascade Manage Azure

1 KEY TERMS

EFFECTIVE DATE:	THIS SERVICE ORDER SHALL GO INTO EFFECT ON THE DATE THE SERVICE IS PROVISIONED AND ONBOARDING OF THE CLIENT ONTO THE SERVICE BEGINS.
INITIAL TERM:	AS SET OUT IN THE QUOTE.
MILESTONES (IF ANY):	AS SET OUT IN THE QUOTE.
SITE(S):	AS SET OUT IN THE QUOTE
DELIVERABLES (IF ANY):	Monthly Reports, detailing tickets raised, patching, AV and backup status.
CHARGES AND PAYMENT TERMS:	AS SET OUT IN THE QUOTE.
CUSTOMER EQUIPMENT (IF ANY):	AS SET OUT IN THE QUOTE.
SUPPLIER EQUIPMENT (IF ANY):	AS SET OUT IN THE QUOTE.
PLAN:	AS SET OUT IN THE QUOTE.

1.1 Kascade is a trading name of Computerworld (Systems) Limited. Throughout this Service Order, references to Kascade shall also include Computerworld (Systems) Limited. Computerworld (Systems) Limited and Kascade are used interchangeably to represent our business and services.

1.2 This Service Order is entered into pursuant to the Quote issued by Kascade (the **Supplier**) to the customer as set out in the Quote (the **Customer**), and the Supplier's terms and conditions contained in the Quote (**Terms**).

1.3 This Service Order is dated on signature of the Quote by both parties.

1.4 Where the Customer receives Microsoft Azure products and/or services from the Supplier (**Microsoft Azure Services**), the Customer has entered into a separate agreement with the Supplier for the supply of the Microsoft Azure Services (**Microsoft Azure Agreement**).

1.5 Where the Customer receives Microsoft Azure Services from a third party supplier, the Customer agrees to transfer the existing subscription to the Supplier on or before the Quote is signed by the parties (**Transfer**). As part of the Transfer, the Customer agrees to:

1.5.1 enter into a separate agreement with the Supplier for the supply of Microsoft Azure Services from Microsoft Azure, which incorporates the Microsoft Azure Terms of Use;

1.5.2 provide the billing entity details to the Supplier so billing responsibility is transferred from the third party supplier;

1.5.3 allow the Supplier to enrol its Microsoft Azure Subscription into MDC; and

1.5.4 grant the Supplier administration access to the Customer's OS.

1.6 The Supplier will supply the Customer with the Kascade Manage - Azure (**Kascade Azure Managed Service**) as per the terms of this Service Order, the Quote and the Terms.

1.7 Unless the context otherwise requires, or otherwise defined in this Service Order, defined terms in this Service Order shall have the same meaning as the defined terms in the Terms and the Quote.

1.8 Save as may be varied by or otherwise set out in this Service Order, Clause 4 to clause 32 of the Terms shall apply mutatis mutandis to this Service Order.

1.9 By accepting the Supplier's Quote, the Customer has agreed to accept and be bound by the terms of this Service Order.

1.10 In the event there is conflict between the Terms and this Service Order, the terms of this Service Order will prevail.

1.11 In the event there is conflict between the Service Order and the Quote, the terms of the Quote will prevail.

2 DEFINITIONS

2.1 The following definitions and rules of interpretation apply in this Service Order:

Annual Service Review	the annual review meeting of the Kascade Azure Managed Service arranged by the Supplier and held between the parties to ensure the Kascade Azure Managed Service is providing value for money alongside discussing and addressing any service deficiencies or improvements to the service.
Application	an application as part of the Microsoft Azure Application Service Plan.
Architecture Design Review	means part of the Supplier's Kascade Azure Managed Service offering the following benefits: • review Microsoft Azure architecture against latest Microsoft Azure best practices and recommendations, available on the Microsoft Azure Environment only; • review of security score and recommendations of security enhancements made by MDC; and • report on findings and recommended actions.
Microsoft Azure Backup	• backups of Azure servers will be taken and monitored on a daily basis; • 30 day retention point; • check backups are available on a Business Day only between the Standard Support Hours; • failure of any Microsoft Azure server backup will be investigated and remediated; • restoration of any Microsoft Azure server will be undertaken only at Customer's request during standard Business Hours or as part of scheduled Kascade Azure Managed Service tests; • all new production VMs will be backed-up unless requested otherwise; and • report indicating backup success/failure.
Azure Hybrid Benefit	as explained at: https://azure.microsoft.com/en-gb/pricing/hybrid-benefit/#overview and https://azure.microsoft.com/en-gb/pricing/hybrid-benefit/#why-azure-hybrid-benefit
Azure Marketplace	means a catalogue of available Virtual Machines and other Azure instances that can be purchased.

Azure Site Recovery	means a native disaster recovery as a service as included in the Other Microsoft Azure Definitions link.
Bad Patch	a software patch released by the Supplier that has an unexpected impact on a system, which may be the result of the patch being faulty. This may expose further vulnerabilities, or it may inadvertently impact another system. This may result in a service going offline and /or a loss of data.
Business Day	day other than a Saturday, Sunday or public holiday in England and Wales when banks are open for business.
Business Hours	means the Supplier's standard business hours between 8am – 6pm on a Business Day.
Chargeable Instance	a chargeable instance is defined as one of the following: • Microsoft Azure VM; • SQL Managed Instance; • Microsoft Azure SQL database logical server (the administrative point for the service); • VM scale set; and • Microsoft Azure Application Service Plan.
CPU	means the central processing unit.
Kascade Azure Architect	means an architect that specialises in architecting solutions which utilise available feature sets.
Kascade ActiveAlert	means the Supplier's monitoring product which monitors overall health of VM OS and Chargeable Instances and Applications.
DR	means disaster recovery support provided by the Supplier as part of the Premium Plan.
Indirect CSP	a Microsoft Azure distributer.
Initial Term	as set out in the Quote.
Intrusion	any intrusion from any third party, malware, exfiltration of Customer Data, malicious code, intrusion through a firewall or virus or physically implemented virus or attack, Trojan, worm and virus, lock, authorisation key or similar device that impairs or could impair the operation of the Kascade Azure Managed Service.

IT Service Management Solutions	means the Supplier's software that allows for tracking of Customer issues and updates through tickets.
Azure Landing Zone	an environment in Azure on which to host workloads which consists of a collection of Azure networks, security policies, logging and access controls.
MDC	means Microsoft Defender for Cloud, included in the Other Microsoft Azure Definitions link.
Microsoft Azure Application Service Plan	as explained at learn.microsoft.com: https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
Microsoft Azure Disaster Recovery	• replication of workloads in the Azure Site Recovery service schedule to the paired region; • monitoring of replication health status; • creation of recovery plan; • annual DR Failover test (as further defined in clause 6.10) to Customer's isolated network; • DR Failover of Customer's environment to secondary region during outage or as directed by Microsoft Azure; and • reprotection and DR Failback of Azure protected resources.
Microsoft Azure Environment	means the hosted cloud platform provided by Microsoft for public and business consumption.
Microsoft Azure Optimisation	means part of the Supplier's Kascade Azure Managed Service offering the following benefits: • scheduled review of your Microsoft Azure Environment to identify opportunities to manage and optimise in the most cost-efficient way using recommendations by CW Azure Architect; • automated resource management which can be turned off when not used/needed by Customer; • right sizing – to ensure deployed resources match the requirements of the workload; • Reserved Instances – to ensure full use is made of Reserved Instances, to save on costs; • licensing – using the most cost effective licensing by ensuring clients have provisioned a VM with the correct minimum licencing for the purpose of the VM; model for your workloads with Azure Hybrid Benefit • Data Retention – ensure the correct tier is being used to match business requirements; and

	• orphaned resources – check for unused or orphaned Microsoft Azure resources, or resources that are no longer required by Customer.
Microsoft Azure Strategy Review	Part of the Supplier's Kascade Azure Managed Service offering a technical strategy meeting with a Supplier CW Azure Architect, which includes: • technology updates; • review of cloud adoption; and • planning for business projects and priorities.
Microsoft Azure Subscription	Customer's new or existing subscription to Microsoft Azure Services. This is the subscription that hosts the Chargeable Instances.
OS	Means the Virtual Machine operating system.
Other Microsoft Azure Definitions	an exhaustive list of Microsoft Azure definitions (which may be updated from time to time), found at the following link https://azure.microsoft.com/en-gb/products/
Plans	Set Premium, Advanced and Standard plans, as defined in clause 0 below.
Point to Site VPN	means a VPN from a Customer to Azure which will allow Customer to access all applicable Azure resources.
PS Rate	the Supplier's professional services rate available on request.
Quote	the unified quote template populated with the Customer's details by the Supplier.
RAM	means random access memory.
Reserved Instance	means an amount of CPU and RAM Customer pays for each month.
RPO	the recovery point objective, being the amount of data loss incurred when failing over to Kascade Azure Managed Service.
RTO	the return to operation, being the time it takes after Kascade Azure Managed Service is invoked for the system to be live and running in the Kascade Azure Managed Service Environment.

Security Alerts	means as explained in the reference guide at https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference).
Security Alerts (definitions of High, Medium and Low) and Incidents	means as included in the Other Microsoft Azure Definitions link.
Service Delivery Manager	means the person(s) responsible for the following in relation to the Kascade Azure Managed Service; • delivery of the Kascade Azure Managed Service; • ensuring the Kascade Azure Managed Service is meeting Customer's expectation; and • ensuring the parties are compliant with the contractual obligations.
Site to Site VPN	means a third party location (such as Customer's office) to another site (which is Azure). It will allow Customer's clients in your premises to access all Customer's resources in Azure as applicable.
SLA	Service Level terms set out in clause 0.
SQL	means structured query language which can be purchased as an application or as an instance in Azure as included in the Other Microsoft Azure Definitions link.
Successive Term	any additional term after the Initial Term of this Service Order, as further detailed in the Terms.
Supported List	means a list of applications supported by the cloud patching system.
Term	means the Initial Term and any Successive Term agree between the parties.
VMs	virtual machines.

3 Service Offering

Standard Plan	For the Standard Plan, the Supplier will provide management for the following components located in the CWC_AZMS (Customer_Name) subscription, available for the Standard Support Hours:
	• break/fix of the Azure Landing Zone, Chargeable Instances and associated core Microsoft Azure components as applicable to the Kascade Azure Managed Service
	• proactive support and maintenance via Kascade ActiveAlert for all VM OS instances
	• deployment of new VM from the Azure Marketplace
	• resizing instances reactively or proactively
	• monitoring and remediation of MDC Security Alerts
	• guest OS patching for VM Instances
	• deployment and Management of Antivirus on all VM workloads
	• annual Architecture Design Review
	• annual Microsoft Azure Optimisation
	• monthly reporting on
	  ○ capacity trends for CPU, RAM and storage (VM Instances only);
	  ○ patching compliance;
	  ○ AV Compliance; and
	  ○ support tickets raised
	• Annual Service Review
	• priority access to future Microsoft Azure workshops, training and events

Advanced Plan	The Advanced Plan includes the same offerings as the Standard Plan, with the following additional features: • fully managed Microsoft Azure Backup for all applicable Chargeable Instances using native Microsoft Azure Backup • 2 Architecture Design Reviews per year • 2 Microsoft Azure Optimisation per Year; and • annual Microsoft Azure Strategy Review

Premium Plan	The Premium Plan includes the same offerings as the Standard Plan and Advanced Plans, with the following additional features: • fully managed Microsoft Azure Disaster Recovery of protected workloads to a secondary region • 4x Architecture Design Reviews per Year • 4x Microsoft Azure Optimisation per Year • 2 Microsoft Azure Strategy Review per Year • P1 priority escalation 24x7

4 SUPPORT HOURS

4.1 **Standard Support Hours** (10x5) Monday – Friday (excluding bank holidays) 08:00 – 18:00

4.2 **Premium Support Hours for P1 only (available on the Premium Plan only)** (24x7) Monday – Sunday (including bank holidays, excluding Christmas day)

5 SERVICE LEVELS

5.1 Support process

5.1.1 The Supplier offers two methods of contacting the Supplier's support team – via telephone or email to the following details:

Telephone	0344 833 0601
Email	support@kascade.co.uk

5.2 Support Service Incident Priority and Response Times

5.2.1 Incident priorities will be recorded as a ticket by the Customer at the time of logging a case, which shall be revised by the Supplier's support team (**Tickets**).

5.2.2 If the Customer is not satisfied with a revised priority of a Ticket, then this will be a matter for negotiation and escalation as required.

5.2.3 Supplier will use reasonable endeavours to ensure that 98% of Tickets are triaged and prioritised within 1 hour of receipt. If the Supplier fails to comply with this obligation on 3 occasions during a calendar month, the Customer shall have the right to terminate this Service Order under clause 14.1.2 of the Terms if the termination notice is received by the Supplier before the end of the following calendar month.

5.2.4 The Supplier will use reasonable endeavours to ensure that 98% of Tickets are resolved within the timeframes according to the Incident Priority table below. If, during a calendar month, the Supplier fails to resolve 3 P1 and/or P2 Tickets within the timeframes according to the Incident Priority table below, the Customer shall have the right to terminate this Service Order under clause 14.1.2 of the Terms, if such termination notice is received by the Supplier before the end of the following calendar month. Where Tickets are awaiting third party input, are being monitored to see if the fix is working, or waiting for a client response, this will pause the resolution time until such time as an appropriate response is received.

5.2.5 Where Tickets are awaiting third party input, are being monitored to see if the fix is working, or waiting for a client response, this will pause the resolution time until such time as an appropriate response is received.

5.3 Support Service Incident Priority & Response Times

5.3.1 Incident priorities will be recorded by the Supplier at the time of logging a case according to the severity of the request.

5.3.2 The Incident Priority table below summarises the fix time SLA

Incident Priority	Description of Priority and Timeframe	Service Level
P1	High Priority: Complete loss of business-critical workload, service, or application.	98% of tickets to be resolved within 4 Business Hours
P2	Medium Priority: Significant issue affecting a non-critical workload, service or application.	98% of tickets to be resolved within 1 Business Day
P3	Low Priority: Minor issue affecting non-critical functionality.	98% of tickets to be resolved within 3 Business Days
P4	General Queries: Advice, Administrative changes, etc.	98% of tickets to be resolved within 5 Business Days

5.4 Incident escalation

5.4.1 Incidents are managed by the Supplier through the IT Service Management Solution. Incidents that move outside SLA are automatically escalated to the relevant Service Desk Manager.

5.4.2 SLA performance is reviewed as part of the Annual Service Review, or on an add hoc basis should a valid need arise, by the Service Delivery Manager.

6 ADDITIONAL TERMS

The following additional terms apply to the provision of the Kascade Azure Managed Service.

6.1 Suppliers systems

6.1.1 The Customer allows the Supplier to add the relevant subscriptions and Chargeable Instances to its various monitoring and management solutions which may change from time to time.

6.2 Costs

6.2.1 Azure consumption charges will be billed under a separate consumption invoice as per the terms of the Microsoft Azure Agreement.

6.3 Microsoft Azure Subscription

6.3.1 Supplier will supply a new Microsoft Azure Subscription which will be named to “CWC_AZMS (Customer_Name)”. Supplier will deploy its base Azure Landing Zone to the Microsoft Azure Subscription which is a collection of best practice policies, security and functionality.

6.3.2 Where Microsoft Azure Subscription is not initially provided by Supplier and is subsequently Transferred to Supplier, Customer will ensure that it has:

6.3.2.1 any existing subscription used to host Chargeable Instances renamed to “CWC_AZMS (Customer_Name)”;

6.3.2.2 enter into a separate agreement with the Supplier for the supply of Microsoft Azure Services from Microsoft Azure, which incorporates the Microsoft Azure Terms of Use;

6.3.2.3 the billing and administration transferred to Supplier so billing responsibility is transferred from the third party supplier; and

6.3.2.4 policies introduced to bring it up to the baseline standards that Supplier would apply to a new Microsoft Azure Subscription, where applicable.

6.3.3 The Microsoft Azure Subscription that has the Chargeable Instances covered by the scope of this Service Order must be provided by the Supplier for the Term of the Service Order.

6.3.4 If a Chargeable Instance is moved out of the Microsoft Azure Subscription then that Chargeable Instance is no longer included in the scope of this Service Order.

6.3.5 The Customer agrees to have the Microsoft Azure Subscription joint owned and managed by the Customer, Supplier and Indirect CSP provider.

6.3.6 The Customer agrees that the Microsoft Azure Subscription is added to and managed by the Suppliers CW ActiveAlert monitoring platform.

6.4 Cancellation

6.4.1 Cancellation of this Service Order does not constitute a cancellation of the Microsoft Azure Agreement.

6.5 Support

6.5.1 Monitoring and support is limited to Chargeable Instances and their associated components located on the Microsoft Azure Subscription.

6.5.2 Supplier will only supply monitoring and support for the OS of any Chargeable Instance. Supplier does not provide any support of Applications installed onto the VM.

6.5.3 Supplier will only manage and support SQL instance's and not the database's themselves nor any third party software that references them.

6.5.4 Should any Site to Site VPN or Point to Site VPN be created for the Customer, Supplier are only responsible for supporting the Azure side of the VPN.

6.5.5 When remediating issues that require purchase of additional services such as larger disks for VMs, Supplier will attempt to contact the Customer to seek authorization twice before electing to remediate, to avoid complex outage situations. The frequency of the attempts to contact the Customer will vary depending on the urgency of the required remediation. The Supplier reserves the right to take discretionary action to remediate issues in an emergency, including in the absence of receiving a response from the Customer.

6.6 Monitoring and alerting:

6.6.1 Critical and error alerts will be automatically logged and remediated. Warning alerts will not be responded too.

6.6.2 The following VM metrics will be included in Kascade ActiveAlert;

- CPU utilisation;
- disk capacity free space;
- memory utilisation; and
- resource availability (is the VM online).

6.6.3 CW will apply a standard metric template to all VM instances.

6.6.4 Customer may change threshold by notifying Supplier to raise to a new threshold in writing to support@kascade.co.uk, and the Supplier will use reasonable endeavours to action the changes within 5 Business Days of receiving notice from the Customer.

6.6.5 Security Alerts when threats are detected are categorized by Microsoft into High, Medium, Low and informational alert categories.

Microsoft Azure's Security Alerts definition include examples for the different categories of Security Alerts which are further detailed on the website, such as:

- **High:** compromised virtual machines communicating with known malicious IP addresses, brute force attack against VMs.
- **Medium:** antimalware being disabled, detection of high risk software.
- **Low:** ransomware indicators, a benign positive or a blocked attack.

6.6.6 Supplier will respond to any High or Medium Security Alerts generated by MDC as may change from time to time.

6.6.7 MDC will incur additional Microsoft Azure consumption charges that will reflect in the Microsoft Azure Agreement charge.

6.7 Azure Landing Zone and other components

6.7.1 Supplier will implement and Azure Landing Zone to a comprehensive secure best practice.

6.7.2 Supplier is not responsible for, and has no liability in respect of, any Intrusion relating to the Service.

6.7.3 Remediation of issues due to any Intrusion will be charged at additional cost as per the Supplier's prevailing PS Rates.

6.8 System Updates

6.8.1 The Customer shall be responsible for ensuring that all Microsoft Azure software is correctly licensed and supported.

6.8.2 Supplier will only deploy new VMs from the Azure Marketplace.

6.8.3 Patching

6.8.3.1 Supplier will patch VM instances using its Cloud patching system (**Patching**). Patching will take place on all supported Windows OS's, along with native Windows applications and supported third party Applications.

6.8.3.2 Patching will be undertaken automatically on a fortnightly basis. The VM instances will be split between two update rings and each ring will be patched during alternate weeks in a fortnightly cycle as follows:

6.8.3.2.1 Ring0 will be patched at approximately 3am on the first Sunday of a given month;

6.8.3.2.2 Ring1 will be patched at approximately 3am on the second Sunday of a given month; and

6.8.3.2.3 each Ring will update then on a fortnightly basis with the 5th Sunday in a given month being skipped.

6.8.4 Supplier is unable to offer alternate dates and times for Patching, however the Customer may exclude VMs from Patching and do this manually instead.

6.8.5 Day 0 software exploits will be Patched as soon as the Supplier releases a patch and it is available within the Supplier's Patching system to deploy.

6.8.6 It is the Customer's responsibility to notify the Supplier of a Bad Patch, who will then mark this and stop the Bad Patch deploying further where possible. The Supplier will then provide reasonable assistance to the Customer to remediate the Bad Patch, either by removing it, or restoring the affected VM from Microsoft Azure Backup (available with Advanced and Premium Plans only).

6.8.7 Except as set out in clause 13.3 of the Terms, Supplier is not responsible for any losses the Customer incurs as the result of a Bad Patch.

6.8.8 If the Customer has applications that fall outside the Supported List, it is the Customer's responsibility to keep these Patched.

6.8.9 Supplier will perform system upgrades on existing VM OS's or deploy new VM's as Applications require from time to time, as instructed by the Customer. Supplier is not responsible for any Application outages due to upgrades.

6.9 Antivirus

6.9.1 The Customer agrees to use the Supplier's antivirus product.

6.9.2 The Supplier will deploy antivirus to each VM, and will work with the Customer to agree a system scan schedule.

6.9.3 The Customer is responsible for notifying the Supplier of any exclusions that may be required for Applications to function correctly.

6.9.4 Antivirus will be installed on each VM created by the Supplier before it is handed to the Customer for Application installation.

6.9.5 The Customer must inform the Supplier in writing by email, of any newly created VM instance so antivirus may be deployed. Failure to do so is a material breach of the Agreement.

6.9.6 Supplier is not responsible for, and has no liability in respect of, any Intrusion relating to the Kascade Azure Managed Service.

6.9.7 Remediation of issues due to any Intrusion will be charged at additional cost as per the Supplier's prevailing PS Rates.

6.9.8 Microsoft Azure Backup (Advanced and Premium only)

6.9.9 Supplier will scope, create and maintain a service schedule for the VM's in scope with frequency and retention requirements.

6.9.10 RTO and RPO are subject to Microsoft Azure Backup service restrictions.

6.9.11 Microsoft Azure Backup will result in higher than usual Azure consumption charges, which will be reflected in the Customer's Microsoft Azure Agreement.

6.10 DR testing (Premium only)

6.10.1 DR is implemented between two or more Microsoft Azure regions.

6.10.2 Supplier will scope, create and maintain a copy of a recovery plan for the Customer to be used in a test or live DR event.

6.10.3 An annual DR test will take place at the Customer's discretion no later than 8 months after this Service Order is live. Customer must provide Supplier with at least one months' notice of the date for an annual DR test.

6.10.4 The annual DR test is optional at the Customer's discretion, however if no test is conducted, Supplier cannot guarantee it will function correctly in a live DR event.

6.10.5 All DR tests will result in higher than usual Azure consumption charges, which will be reflected in the Customer's Microsoft Azure Agreement.

6.10.6 Failover for DR testing can only be instructed by authorised named contacts which have been approved by Supplier, who can supply the Failover password to the Supplier. The Customer will agree the password on onboarding of the Kascade Azure Managed Service and may then change from time to time on notice to the Supplier in writing.

6.11 DR Failback/Failover

6.11.1 Supplier will Failover either planned as agreed with the Customer, or ad hoc as directed by the Customer for a DR event (**Failover**).

6.11.2 Supplier will work with the Customer to Failover back to the original region after testing as directed by the Customer, or when the DR event has been cleared (**Failback**).f

6.11.3 Supplier will use reasonable endeavours to rectify any issues preventing a guest OS from booting up successfully after a DR test Failover or a live Failover or Failback.

6.11.4 Supplier is not responsible for any application remediation

6.11.5 The Customer is responsible for all application remediation prior, during or following a Failover event, be that planned or unplanned.

6.11.6 A Failover, whether Test or Live, can only be authorised by named contacts within the client and the supply of an agreed password. The named contacts and the password will be agreed and recorded during service onboarding and can subsequently be changed by the client upon written request.

6.12 Billing

6.12.1 The Customer may increase the number of Chargeable Instances protected by the Kascade Azure Managed Service at any point during the Initial Term (or any subsequent Term) of the Service Order by purchasing an additional Pack.

6.12.2 Each pack including the base pack provides coverage for up to 5 chargeable instances.

6.12.3 The Customer may not reduce the number of Packs below the initial amount as set out in the Quote for the duration of the Term.

6.12.4 The Customer may, on giving the Supplier one months' written notice prior to the end of the relevant Term, request to reduce the number of Packs in use for any agreed Successive Term.

6.12.5 The Customer must ensure they purchase a sufficient amount of Packs to cover the number of Instances protected by the Kascade Azure Managed Service.

6.12.6 A Customer must buy a Base Pack and then Expansion Packs as required. Details of these Packs are set out as follows:

6.12.6.1 Base Packs: This covers the Azure Landing Zone components plus 5 Chargeable Instances:

Base SKU	Service
CWC_AZMS_SB	Standard Plan
CWC_AZMS_AB	Advanced Plan
CWC_AZMS_PB	Premium Plan

6.12.6.2 Expansion Packs: covers up to 5 additional Chargeable Instances:

VM Packs	Service
CWC_AZMS_S5E	Standard 5 VM Pack

CWC_AZMS_A5E	Advanced 5 VM Pack
CWC_AZMS_P5E	Premium 5 VM Pack

6.12.7 Customer may not mix and match Premium, Advanced or Standard Plans.

6.12.8 Supplier reserves the right to apply additional Packs to the order should it be discovered the Customer has added additional Chargeable Instances to the Azure landing zone without informing the Supplier.

6.13 Description of Personal Data Processing

6.13.1 The data processing activities carried out by Supplier are described as follows:

6.13.1.1 Subject matter

For the purposes of providing the Kascade Azure Managed Service to the Customer.

6.13.1.2 Duration

The Term of the Agreement until the deletion of the personal data in accordance with the Agreement.

6.13.1.3 Nature and purpose

For the purposes of providing the Kascade Azure Managed Service to the Customer.

6.13.1.4 Data categories

The categories of personal data which are provided by the Customer to the Supplier for the Kascade Azure Managed Service.

6.13.1.5 Data subjects

The personal data of the Customers' employees and/or authorised users which is provided to the Supplier for the Kascade Azure Managed Service.

6.13.2 In accordance with clause 2.6 and clause 2.9 of Schedule 1 of the Terms, the Customer consents to the appointment of Binary Fortress Software as a Data Controller. Any personal data processed by Binary Fortress Software will be processed in accordance with Binary Fortress Software's privacy policy (https://www.checkcentral.cc/Privacy/).