PROACT

G-Cloud 15

Monitoring or Managed Service for Azure Public Cloud as a service

PROACT

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
03/12/2025	Colin Abram	V1	Document Upload

PROACT

Monitoring or Managed Service for Azure Public Cloud as a service

Proact provide 24x7x365 monitoring and management services via our Service Operations. Proact's Service Operations includes support for a range of device hardware, platforms, software and systems. All monitoring and support activities are performed remotely via secure internet connectivity.

Service Operations - Standard provides monitoring and includes the following deliverables:

- 24x7x365 Proact service desk and automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Event and incident management.
- Incident response and action of pre-agreed changes
- Performance & capacity Monitoring
- Root cause investigation assistance
- Security aligned operational controls

Service Operations – Premium provides management in addition to monitoring for device hardware, platforms, software and systems:

- 24x7x365 Proact service desk and automated monitoring of devices
- Self-service support and self-service monitoring portals
- Break-fix fault co-ordination and resolution
- Event, incident and problem management.
- Incident response, action of pre-agreed changes, troubleshooting and resolution
- Proactive root cause analysis and prevention
- Security aligned operational controls
- Performance and capacity optimisation
- Change, patch and configuration management
- A named Service Delivery Manager to co-ordinate delivery and provide regular customer reports

Proact provide support for the following technology areas as part of the Monitoring and Management services:

- Storage systems and associated software
- Hypervisors
- Server Operating Systems
- Network appliances and devices (Firewalls, Switches, Routers, Load Balancers)
- Backup software and associated hardware platform
- Public Cloud
- Azure Virtual Desktop
- Workspace software
- M365, Intune, Entra ID and Active Directory

This document contains the following appendices detailing the service definitions for the Monitoring and Management services:

PROACT

Appendix 1 – Service Operations

1.1 - Service Overview

Proact's Service Operations provides the Customer with a 24/7 remote monitoring, support and management solution for a range of hardware, software and systems.

All monitoring, support and management activities are performed through secure links.

Service Operations are delivered in two different levels:

- Standard Operations: Proact provides monitoring, and active incident resolution, with pre-agreed actions, without requiring customer interaction.
- Premium Operations: In addition to Standard, Proact provides incident response, resolution and performs operational activities on Customer request.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Respond to reasonable service requests for relevant information and advice.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Deliverables for Standard Operations are in addition to the above deliverables listed as 'General'

Standard - Standing Charge
Proact shall: • Provide the Customer administrator with access to the Proact monitoring portal. • Provide an encrypted tunnel over the internet to secure service traffic. • Provide internet bandwidth for the transfer of service traffic. • Deploy remote monitoring applications to collect statistics/events/alerts for CIs. • Deploy remote management applications to manage CIs. • Create monitoring profiles to meet the Customer's threshold requirements. • Work with the Customer to define appropriate pre-agreed actions for incident resolution. • Escalate incident alerts to its technical teams for review. • Respond to incidents alerts with appropriate pre-agreed actions to attempt resolution. • Where pre-agreed actions are inappropriate or are ineffective, escalate to the Customer for resolution. • Provide critical fault alert, vendor co-ordination, incident support and hardware break-fix. • Provide a service review report.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Provide a network administrator to configure and troubleshoot service traffic.
- Provide service accounts and passwords/keys with privileges to allow Proact to manage/monitor the CIs.
- Manage CIs within the Customer's site.
- Work with Proact to define appropriate pre-agreed actions for incident resolution.
- Resolve incidents where pre-agreed actions are inappropriate or ineffective.
- Ensure CIs retain historic log data and make log data available to Proact for troubleshooting.
- Provide sufficient licenses for the CIs to achieve the level of functionality the Customer requires.
- For hardware CIs, provide a minimum of a break-fix vendor support contract.
- For compatible devices, configure 'dial home' diagnostics to report to Proact's service desk.
- Provide 'on demand' remote access to managed CIs, when required by Proact.
- Provide, deploy and manage server/cloud instances to host the remote monitoring/management applications.
- License and apply vendor/security updates to OSs hosting the remote monitoring/management applications.
- Install vendor patches/security updates to the CIs.
- Install CI software major version upgrades to introduce functionality or remain in vendor support.
- Inform Proact of planned maintenance or other operations that may impact the service.
- Be billed directly by the cloud provider for any public cloud resources consumed.

Green elements are specific to Standard Only, and are not required with Premium.

Deliverables in Orange are for Premium Operations only and are in addition deliverables listed as 'Standard' (in black) which are also shown here.

Premium - Standing Charge
Proact shall: • Provide the Customer administrator with access to the Proact monitoring portal. • Provide an encrypted tunnel over the internet to secure service traffic. • Provide internet bandwidth for the transfer of service traffic. • Deploy remote monitoring applications to collect statistics/events/alerts for CIs. • Deploy remote management applications to manage CIs. • Create monitoring profiles to meet the Customer's threshold requirements. • Provide critical fault alert, vendor co-ordination, incident support and hardware break-fix. • Provide a service review report. • Manage CIs within the Customer's site using secure remote monitoring applications. • Escalate incident alerts to its technical teams for investigation and resolution. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Provide a major incident report, where required. • Provide reasonable problem management. • Provide incident trend analysis. • Organise a quarterly service review meeting. • Review vendor patch/security updates monthly and install approved patches within thirty days. • Inform the Customer of scheduled patch/update tasks, prior to deployment. • Provide patch status reports as part of scheduled service review reports. • Review DR/redundancy test plan provided by the customer. • Perform agreed DR/redundancy test actions for CIs during normal Proact business hours.
The Customer shall: • Provide sufficient internet bandwidth for the transfer of service traffic. • Provide an external IPv4 public IP address for the creation of the encrypted tunnel. • Provide a network administrator to configure and troubleshoot service traffic. • Provide service accounts and passwords/keys with privileges to allow Proact to manage/monitor the CIs. • Ensure CIs retain historic log data and make log data available to Proact for troubleshooting. • Provide sufficient licenses for the CIs to achieve the level of functionality the Customer requires.

- For hardware CIs, provide a minimum of a break-fix vendor support contract.
- For compatible devices, configure 'dial home' diagnostics to report to Proact's service desk.
- Provide 'on demand' remote access to managed CIs, when required by Proact.
- Provide and manage servers/cloud instances to host the remote monitoring/management applications.
- Install CI software major version upgrades to introduce functionality or remain in vendor support.
- Inform Proact of planned maintenance or other operations that may impact the service.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Nominate named individuals to engage with Proact on the approval and timing of changes.
- Work with Proact to agree predefined actions for common types of incidents.
- Ensure CI's vendor patch/security updates are up to date prior to service commencement.
- Assign CIs to separate patching groups to allow patching to be staged for reliability testing.
- Notify Proact of any changes to the patch/update task at least eight working hours prior to commencement.
- Validate the functionality of all CIs following a patch update.
- Provide thirty day's notice of the intention to perform a DR/redundancy test for CIs.
- Provide Proact with a DR/redundancy test plan for all CIs seven working days prior to testing.

The following elements are out of scope of the service:

- DR/redundancy testing performed outside of local business hours.

1.2 - Storage Operations Service Definition

Premium - Standing Charge
Proact shall: • Manage logical storage units, presentations, and storage efficiency features. • Manage physical components including disks, arrays etc. • Manage storage network, authentication, performance, and encryption configurations.
The Customer shall: • Replace 'customer replaceable components' such as disk drives at the vendor's or Proact's request.

Premium - Replication
Proact shall: • Manage synchronous and asynchronous replication between storage devices.

Premium - Hosts
Proact shall: • Use vender server software to manage system backup and replication between storage devices. • Use vendor software to manage host access to the storage solution.

Premium - SAN
Proact shall: • Manage and present storage device snapshots or clones. • Manage licensing, quotas and statistics through vendor server software.

Premium - NAS
Proact shall: • Manage and present storage device snapshots or clones. • Manage licensing, quotas, and statistics through vendor server software. • Manage OS authentication and file locking settings. • Manage distributed file system configuration and replication.

Premium - Object
Proact shall: • Manage licensing, quotas, and statistics through vendor server software. • Manage lifecycle, erasure coding, and replication policies. • Manage OS authentication and file locking settings.

Premium - Switches
Proact shall: • Manage connectivity between switches and storage devices. • Manage ports and grouping/zoning for fibre channel (FC) or fibre channel over Ethernet (FCoE) switches.

1.3 - Server Operations Service Definition

Premium - Standing Charge
Proact shall: • Manage OS's local authentication and remote administration access. • Manage logging, network, and license configuration. • Manage user/group management, encryption, and certificate configuration. • Manage local storage and file systems.
The following elements are out of scope of the service: • Management of central authentication or administration systems, such as GPO, Active Directory or EntraID.

Standard - Physical
Proact shall: • Respond to hardware alerts from a separate 'out of band' IPMI management interface.
The Customer shall: • Ensure each physical system has a separate 'out of band' IPMI management interface.

Deliverables in Orange are for Premium Operations only and are in addition deliverables listed as 'Standard' (in black) which are also shown here.

Premium - Physical
Proact shall: • Respond to hardware alerts from a separate 'out of band' IPMI management interface. • Manage network adapters and fibre channel over Ethernet transport (FCoE). • Manage intelligent platform management interface (IPMI) configuration. • Manage trusted platform module settings. • Manage BIOS and boot storage configuration for physical/blade systems.
The Customer shall: • Ensure each physical system has a separate 'out of band' IPMI management interface.

Premium - Clustering
Proact shall: • Manage native clustering, networking, and shared storage at the OS level. • Manage backup and synchronisation of cluster configuration. • Manage load balancing of resources between the cluster nodes.

Premium - Antivirus
Proact shall: • Provide and centrally manage Antivirus (AV) software. • Schedule AV scanning and configure quarantining. • Escalate AV alerts, that cannot be handled by the AV software, to the Customer's administrators. • Configure and manage OS security settings with the OS vendor's native tooling.
The Customer shall: • Nominate named individuals to received AV software alerts.

Premium - File & Print
Proact shall: • Manage authentication security, access control and file locking mechanisms. • Manage native SMB and NFS connectivity. • Manage file serving, quota management and distributed file systems. • Manage print server and network printing configuration.

1.4 - Hypervisor Operations Service Definition

Standard - Standing Charge
Proact shall: • Respond to hardware alerts from a separate 'out of band' IPMI management interface.
The Customer shall: • Ensure each physical system has a separate 'out of band' IPMI management interface.

Deliverables in Orange are for Premium Operations only and are in addition deliverables listed as 'Standard' (in black) which are also shown here.

Premium - Standing Charge
Proact shall: • Respond to hardware alerts from a separate 'out of band' IPMI management interface. • Using the hypervisor central management application, manage hypervisor OS tools within compatible VMs. • Create new VMs upon request by using templates or cloning existing VMs. • Monitor hypervisor storage and alert on threshold breaches. • Work with the Customer to utilise their existing storage capacity for growth.
The Customer shall: • Ensure each physical system has a separate 'out of band' IPMI management interface. • Maintain sufficient expansion capacity to cope with storage threshold breaches. • Work with Proact to extend storage in the event of a threshold breach.

Premium - Data Protection
Proact shall: • Manage replication with the native hypervisor disaster recovery application. • Create replication policies and schedules and VMs. • Make changes to VM assignment, replication policies, and schedules, upon request.
Customer shall: • Define VMs that require replication and inform Proact of changes.

- Work with their application vendor to achieve application consistency.

Premium - Backup & Restore

Proact shall:

- Perform restore tasks using the hypervisor snapshot backup capabilities.

1.5 - Network Operations Service Definition

Premium - Standing Charge

Proact shall:

- Manage Ethernet ports, trunk/uplink ports and Ethernet aggregation.
- Manage Ethernet device access and syslog/external log transfer.
- Monitor and report on free ports, port errors and utilisation.

Premium - Access Switch

Proact shall:

- Manage VLANs, STP, VoIP, port protection, and switch stacking.

Premium - Distribution Switch

Proact shall:

- Manage VLANs, STP, VoIP, port protection, and switch stacking.
- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage QoS and next hop resolution protocols, e.g. HSRP, VRRP.
- Manage dynamic routing protocols – RIP, OSPF & EIGRP.
- Manage route maps, policies, port security, MACsec, IPMG, and PIM snooping

Premium - Core Switch

Proact shall:

- Manage VLANs, STP, VoIP, port protection, and switch stacking.
- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage QoS and next hop resolution protocols. e.g. HSRP, VRRP.
- Manage dynamic routing protocols – RIP, OSPF & EIGRP.
- Manage routing with border gateway protocol (BGP) for up to 2 neighbours.
- Manage IPv6 tunnelling, MPLS, L2/3-VPN, IP-fabric (eVPN/VXLan) and VRF.
- Manage Route maps & policies, port security, MACsec, IPMG, PIM snooping.
- Manage 802.1x identity management and PIM (sparse mode and bidirectional).

Premium - Branch Router

Proact shall:

- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage QoS and next hop resolution protocols. e.g. HSRP, VRRP.
- Manage dynamic routing protocols – RIP, OSPF & EIGRP.
- Manage routing with border gateway protocol (BGP) for up to 2 neighbours.
- Manage ACL/firewall, DMVPN, VRF-lite, NetFlow, IGMP and PIM snooping.

Premium - Enterprise Router

Proact shall:

- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage QoS and next hop resolution protocols. e.g. HSRP, VRRP.
- Manage dynamic routing protocols – RIP, OSPF & EIGRP.
- Manage routing with border gateway protocol (BGP) for up to 2 neighbours.
- Manage IPv6 tunnelling, MPLS, L2/3-VPN, IP-fabric (eVPN/VXLan) and VRF.
- Manage ACL/firewall, DMVPN, VRF-lite, NetFlow, IGMP and PIM snooping.
- Manage multihoming, BGP full internet and PIM (sparse mode and bidirectional).

Premium - Branch Firewall

Proact shall:

- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage firewall high availability, DNS, NTP, firewall rules (ACL/NAT) and IPS.
- Manage remote access encryption & site to site VPN.

Premium - Enterprise Firewall

Proact shall:

- Manage DHCP/v6, DHCP Snooping, IPv4/v6. VLAN sub-interfaces.
- Manage dynamic routing protocols – RIP, OSPF & EIGRP.
- Manage routing with border gateway protocol (BGP) for up to 2 neighbours.
- Manage firewall high availability, DNS, firewall rules (ACL/NAT) and IPS.
- Manage remote access SSL, NTP client and site to site VPN.
- Manage multicast support, NTP server and LDAP firewall rules.
- Manage anti-malware, deep packet inspection, IPS and anti-virus.
- Manage URL filtering, SSL/TLS proxy/certificates and multi-context/virtual instances.

1.6 - Backup Operation Service Definition

Standard - Standing Charge

The Customer shall:

- Provide Proact with full administration rights to the backup application.

Deliverables in Orange are for Premium Operations only and are in addition deliverables listed as 'Standard' (in black) which are also shown here.

Premium - Standing Charge

Proact shall:

- Manage the backup environment CI's configuration and licensing.
- Monitor, alert and report on individual backup jobs daily.
- Manage backup jobs and schedule in-line with Customer requirements.
- Work with the Customer to resolve failed backup jobs.
- Perform data restores for CIs, upon request.
- Manage logging, reporting, and alerting.
- Manage backup storage and client configuration.
- Manage users, authentication, privileges, and encryption.
- Utilise the Customer's pre-built software packages to perform remote client deployment, where available.
- Work with the Customer to assist in the creation of pre-built software packages.
- Perform software upgrades to the backup software installed from time to time.
- Extend backup storage capacity within the backup software when thresholds are breached.

The Customer shall:

- Provide Proact with full administration rights to the backup application.

• Work with Proact to resolve failed backup jobs. • Confirm the validity and consistency of restored data. • Administer backup users within Active Directory or other authentication systems. • Provide pre-built software packages to allow Proact to perform backup client deployment. • Test deployment of pre-built software packages and confirm compatibility. • Perform upgrades on backup hardware and firmware, where required. • Ensure sufficient physical storage capacity is available to extend backup storage capacity.
The following elements are out of scope of the service: • Performing 'Bare Metal' restores to new hardware without an existing OS or backup agents installed.

Premium - Archive
Proact shall: • Manage archive tasks, schedules, and retention policies. • Manage self-service recovery of archive data through stubs or restore tasks. • Provide the ability for users to erase selected archive content, upon request.

Premium - Data Protection
Proact shall: • Manage continuous data protection (CDP) replication tasks.

Premium - End User Devices
Proact shall: • Manage backup of Customer end-user devices via the internet. • Provide Customer end-users with access to a self-service restore interface.
The Customer shall: • Be responsible for end-user authentication, administration, and device management.

Premium - Tape
Proact shall: • Utilise the Customer's tape hardware to store backup data. • Make request to the Customer to perform tape handling tasks.
The Customer shall: • Perform, or appoint a 3rd party to perform, physical media and cleaning media tape handling tasks. • Provide sufficient tape media/cleaning media and replace aged media, where required.

1.7 - Public Cloud Operations Service Definition

Premium - Standing Charge
Proact shall: • Monitor resource health status, availability, identity, and access management alerts. • Manage public cloud access roles and identities • Limit access to the public cloud management portal through limited public IP or multi-factor authentication.
The Customer shall: • Have and maintain a valid public cloud subscription. • Provide access to the public cloud platform/network. • Utilise the public cloud providers native identity and access management tooling. • Be responsible for access keys stored within the public cloud key vault.

- Limit access to the public cloud management portal through limited public IP or multi-factor authentication.
- Inform Proact of changes that may impact security of the cloud platform.

Public Cloud Landing Zone Service Definition

Premium - Workloads
Proact shall: • Provide the agreed Landing Zone Environment (LZE), prior to service commencement. • Monitor/manage the LZE with Infrastructure as Code (IaC) principles. • Manage CIs and apply changes in-line with the agreed LZE, during business hours. • Provide a Public Cloud Management Platform (PCMP) within the cloud provider. • Utilise the PCMP to manage/develop and update IaC code modules. • Link the PCMP to the customer's LZE to allow LZE monitoring/management and for IaC deployment. • Manage virtual networks, hubs, WAN, and subnets • Manage virtual network security groups and application security groups. • Manage security policy, cost control, and resource configuration. • Manage external access to cloud services and key vaults. • Manage native firewalls (up to layer 3) • Follow-up maintenance alerts that could have impact on business services • Perform monthly code drifting check and report on unexpected environment changes. • Provide a quarterly cost control report and recommendations for possible cost savings. • Provide a quarterly report on unused reservations to optimise reserved resource usage. • Inform the Customer of deviations from Proact's best practice. • Change the LZE, following a written Customer request, as part of a Contract Change.
The Customer shall: • Remediate unexpected environment changes found in the code drifting check. • Provide Proact's PCMP with access and sufficient privileges to monitor/manage the Customer's LZE. • Provide a written request for changes to the LZE, where required.
The following elements are out of scope of the service: • Changes to the environment performed outside of local business hours. • Access to, or use of, the IaC code modules Proact use within the LZE in strictly prohibited.

Premium - Virtual Machine
Proact shall: • Manage the configuration of VMs hosted within the Customer's Workloads. • Monitor VM health status and alert on threshold breaches. • Resizing virtual hardware and disk capacity, upon request. • Manage native backup storage.
The Customer shall: • Manage and monitor the OS and software running within the VM.

Premium - Backup
Proact shall: • Monitor, alert and report on individual backup jobs daily. • Manage backup jobs and schedule in-line with Customer requirements. • Perform data restores for CIs, upon request. • Deploy backup agents for CIs, where applicable. • Work with the Customer to resolve failed backup jobs. • Perform two scheduled restore tests each year, not overwriting Customer data. • Assume any recent successful comparable restore will be classed as a successful test restore.
The Customer shall: • Work with Proact to resolve failed backup jobs.

• Provide restore target resources for restore requests and test restores. • Confirm the validity and consistency of restored data. • Confirm that all backup-capable resources that require protection are included in the backup.

Premium - Application Gateway
Proact shall: • Monitor the application gateway health status and alert on threshold breaches. • Manage application gateway configuration. • Manage backup and restoration of the application gateway configuration.
The Customer shall: • Providing application-specific configurations for setting up the application gateway.

1.8 - Service Level Agreement

1.8.1 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents **within 30 minutes**. A P1 incident is: a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of **15%** of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents **within 1 working hour.** A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of **5%** of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents **within 4 working hours.**

	A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents **within 8 working hours.** A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within **8 working hours** from when authorised**.** A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within **8 working hours** from when authorised**.** A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The C must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within **4 hours** of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of **15%** of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests **within 8 working hours.** A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer.

	'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.9 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name
LogicMonitor

1.10 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be either monitored or managed by Proact, as set out in the Contract.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Landing Zone Environment	The Landing Zone Environment (LZE) defines the overall scope of the public cloud environment approved by Proact and the Customer. The LZE relates to the entire environment managed by Proact and includes; Identity and access management, data security & governance, cost control, network design, application workloads/VMs, and all associated resources. The LZE must be based upon the Microsoft Well-Architected Framework (WAF) and Cloud Adoption Framework principles and conform to Proact's best practice. At any point during the Contract, the Customer may request a change to the LZE to meet new requirements. Such changes to the LZE will be adjusted as part of a Contract Change.
Workload	A Workload relates to a specific application held within the Customers' LZE. The customer may present a single application multiple times; Production, Test, Development, etc. Each application presented will be charged for each individual Workload. For more complex applications, where the number of network security groups or subnets per Workload exceeds 1.8:1, additional empty Workloads will be assigned and subject to applicable charges.

PROACT

Appendix 2 - Service Operations for Modern Workspace - Entra ID and Active Directory

2.1 - Service Overview

Entra ID is the front door to cloud resources. Our Entra ID and Managed Active Directory service ensures the identity infrastructure is secure, compliant, and optimised, freeing local IT teams whilst giving the Customer business seamless and reliable access control.

Proact's Entra ID service offers 24/7 monitoring, incident response, and change management, reducing downtime and catching misconfigurations before they become security risks.

The support model is structured to operate between Proact and the Customer's IT team, while end-user support, ensuring employee productivity, is provided by those who know the users best: the Customer's IT team. Proact delineates responsibilities between end-user support and tenant administration to ensure smooth and efficient operations.

Customer: End-user support

Scope: The Customer is responsible for all user-specific Entra and AD operations, including application access, permissions, and device management for individual users.

Proact: Tenant and Workspace Administration

Scope: Proact handles operations related to Entra / AD configurations and incidents where the symptoms involve multiple users or configurations beyond a single end-user's access.

Escalation: If the issue is related to tenant-wide settings or service beyond our control, Proact will escalate to the Customer Tenant Cloud Solution Provider (CSP).

2.2 - Entra ID Management

Proact shall:

Manage the following Microsoft Entra ID platform features to support secure identity and access management across cloud and on-premises environments:

- Core IAM: SSO, MFA
- Premium controls: hybrid access, privileged identity management, conditional access
- Application Authentication setup: OAuth/SAML
- User Authentication configuration: Passwords, passwordless (Windows Hello, passkeys, FIDO2), certificate-based.
- External identity: B2B scenarios (e.g Configuration of lighthouse)
- Device & app management: Monitoring, and domain services

The Customer shall:

Retain all responsibilities related to internal policy, organization-specific decisions and users & groups.

Approve requests, access changes, or elevated privileges, user and group provisioning, access within third-party or line-of-business apps integrated with Entra ID.

The following elements are out of scope of the service:

Providing reports on account changes, login activity, admin actions and EDR Solutions - These elements are available with Proact's Security Operations services.".

Projects requiring Architecture & Expert-Level reconfiguration including, but not limited to the following, are out of scope and would require a separately costed and contracted Proact Professional Services engagement:

- Designing hybrid identity strategies
- Planning Zero Trust architectures
- Migration from on-prem AD to cloud-native Entra ID

2.3 - Azure AD Connect

Proact shall:

Integrate on-premises directories with Azure AD providing a common identity and enhanced security features for accessing both cloud and on-premises resources.

Investigate / remediate any Synchronisation errors, where access to AD is not required.

Perform any OU filter changes as necessary

Perform AD Connect updates as required to implement bug fixes

The Customer shall:
Define the OUs and maintain users and groups in accordance with the synchronisation structure

The following elements are out of scope of the service:
Changes requiring access to Active Directory are available within Proact's Service Management for Active Directory service.

2.4 - Active Directory

Proact shall:
Maintain the on-premises directory service that provides centralised authentication, authorization, and management of users, devices, and resources within a Windows network environment, including the following elements:

Domain Health Management
Replication topology, domain controller health, and event logs
Alerting on and resolving health AD issues
DNS and DHCP (If AD-integrated)
Managing AD-integrated DNS zones and records
Ensuring reliable name resolution for domain services
Group Policy Object (GPO) Management
Implementing and updating standard GPOs (e.g. password policies, desktop restrictions)
OU (Organizational Unit) Administration
Managing Proact managed objects within existing OU structures
Backup AD State (for Domain Controllers)
Backing up system states for AD recovery (to local share)

The Customer shall:
Retain all responsibilities related to internal policy, organization-specific decisions and users & groups.
Deciding password expiration policies, security group naming conventions, access governance standards, user and group provisioning.

The following elements are out of scope of the service:
Certificate Services
Patch and Update Maintenance for Domain Controllers is available in Proact Service Management for Servers contract in operation.
Backing up system states for AD recovery to third party systems is available in Proact Service Management for Servers.
Providing reports on account changes, login activity, admin actions and EDR Solutions is available in Proact Service Operations for Security.
Projects requiring Architecture & Expert-Level reconfiguration including, but not limited to the following, are out of scope and would require a separately costed and contracted Proact Professional Services engagement:
Forest level updates and changes
Creation of additional domains
Active Directory flattening/consolidation/extension
Migration from on-prem AD to cloud-native Entra ID

2.5 - Service Level Agreement

2.5.1 - Response Time Service Levels

Definition	Description

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: • a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or • an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or • an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges for the directly affected service.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges for the directly affected service.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.

Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

2.6 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name

PROACT

LogicMonitor

PROACT

Appendix 3 - Service Operations for Modern Workspace – M365 and Intune

3.1 - Service Overview

Proact's managed service for Microsoft 365 (formerly Office 365) is designed to ensure a Customer's Microsoft tenant maintains a high level of security, governance, and system reliability.

The support model is structured to operate between Proact and the Customer's IT team, while end-user support, ensuring employee productivity, is provided by those who know the users best: the Customer's IT team. Proact delineates responsibilities between end-user support and tenant administration to ensure smooth and efficient operations.

Customer: End-user support

Scope: The Customer is responsible for all user-specific Entra and AD operations, including application access, permissions, and device management for individual users.

Escalation: If a user issue goes beyond the Customer's ability to resolve (e.g. device or software application failures), it can be escalated to their CSP or the appropriate software or hardware vendor. Where the issue is related to tenant or workspace management, it can be escalated to Proact.

Proact: Tenant and Workspace Administration

Scope: Proact handles operations related to the M365 tenant workspace and incidents where the symptoms involve multiple users or configurations beyond a single end-user's workspace.

Escalation: If the issue is related to tenant-wide settings or service beyond our control, Proact will escalate to the Customer Tenant CSP (Cloud Solutions Provider)

3.2 - Microsoft 365 – Core Platform Management

Proact shall:

Assist with the Definition, Creation and ongoing management of Tenant-level tasks specific to configuration and security ensuring the Customer tenant is efficiently protected, including:
- Tenant Creation
- Assign/remove licenses
- License usage optimization
- MFA enforcement policies – **(as relates to M365 Access)**
- Single sign-on (SSO) to Azure & Microsoft 365 **(as relates to M365 Access)**
- Self-service password reset for cloud users – **(as relates to M365 Access)**

The Customer shall:

Focus on helping users effectively access the Microsoft 365 apps and services.

Troubleshoot individual application and access issues, device setup and configuration, printing and local IT support, user guidance and training.

The following elements are out of scope of the service:

Power Platform (Power BI, Power Automate, Power Apps)

Microsoft Dynamics

Exchange Online (Email & Calendar) Management

Proact shall:

Provide assistance with the Microsoft Exchange Online service at the tenant level, such as initial setup, configuration and policy governance, including:
- Policy Creation and amendment

Mail flow rules (transport rules)
Spam/phishing filter policies
Investigation / remediation of mail delivery issues
Add / remove blocked & Allowed senders
Changes to mail Connectors & Smart hosts

The Customer shall:

Manage individual users access and utilise the Exchange online email services, including:
Troubleshooting email issues on end user devices (sync errors, spam filtering, missing emails).
Create Room Mailboxes representing physical locations
Managing mailbox settings (rules, delegation, out-of-office responses).
Creation and maintenance of shared mailboxes and distribution lists.

3.3 - Microsoft Teams (Collaboration & Communication) Management

Proact shall:

Assist with management of Microsoft teams, advise, recommended and setup configuration as per best practice, including:
Managing Teams policies, governance, and compliance
Configuring security settings (guest access, permissions, conditional access)
Provisioning teams, channels, and external collaboration settings
Monitoring usage analytics

The Customer shall:

Troubleshoot call quality and connectivity issues, assist users with chat, file sharing, and meeting setup.
Provide support for Teams Phone System and integrations

The following elements are out of scope of the service:

Conference lines and VoIP
Teams Meeting Rooms equipment
Backup, available as a separate Proact Backup service.

3.4 - SharePoint Online (Document Management & Intranet) Management

Proact shall:

Actively assist in incident management of SharePoint Online
Provide reports on site usage statistics if required by the Customer.

The Customer shall:

- Manage end user permissions, sharing and sync issues.

The following elements are out of scope of the service:

Backup, available as a separate Proact Backup service.

3.5 - OneDrive for Business (Cloud Storage & Sync) Management

Proact shall:

Monitor usage and access controls
Manage Integration of OneDrive with other Microsoft 365 services
Actively assist in incident management of SharePoint Online

The Customer shall:

Troubleshoot sync issues, assist with file recovery, provide guidance on sharing and collaboration.

The following elements are out of scope of the service:
Backup, available as a separate Proact Backup service.

3.6 - Intune (Device Security & Compliance Management

Proact shall:
Ensure tenant level device security, compliance, and management, including:
- Configuring enrolment policies to suit corporate devices.*
- Managing device configuration profiles*
- Creating conditional access to ensure only compliant and trusted devices can access sensitive Microsoft 365 resources.
- Managing Windows Update Rings
- Deploying OS and application updates to prevent security vulnerabilities.
- Configuring application distribution where an Intune distribution guide is provided by the vendor.

The Customer shall:
Provide end user device support, such as, end user device enrolment, device setup, management and access, remote Wipe & Lost assistance.

The following elements are out of scope of the service:
Troubleshooting of third party (third party = not Microsoft) application distribution or update issues
Mobile and tablet devices are excluded, Proact shall only manage windows devices.
Backup, available as a separate Proact Backup service.

3.7 - Defender for Endpoint (Microsoft 365 E3 Plan 1) Management

Proact shall:
Provide foundational protection and standardised secure operations for Defender for Endpoint via Microsoft 365 Defender, including:
- Device onboarding and baseline policy management
- Updates to exclusion lists within the Defender for Endpoint portal.
- Configuration of centralised alerts to Customer ticketing systems

The Customer shall:
Provide basic support for Defender alerts and device notifications
Guidance on handling blocked files and safe browsing practices
Security Incidents and response.

The following elements are out of scope of the service:
Microsoft 365 E5 + Microsoft Defender for Endpoint with Microsoft Sentinel or Microsoft 365 Business Premium.
- Advanced detection, EDR, and 24x7 vulnerability management requires Proact MDR Security Operations.

3.8 - Service Level Agreement

3.8.1 - Response Time Service Levels

Definition	Description

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: • a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or • an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or • an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges for the directly affected service.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges for the directly affected service.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.

Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

3.9 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name

PROACT

LogicMonitor

Appendix 4 - Service Operations for Modern Workspace – AVD

Modern Workspace Service Operations refers to a structured, ongoing set of operational and support services provided by a Proact to ensure the performance, reliability, and cost-efficiency of The Customer's digital workspace environment. This typically includes platforms like Azure Virtual Desktop (AVD), Citrix, or other virtual desktop infrastructures (VDI).

It is formalised within this Managed Service Agreement, which outlines the scope, deliverables, responsibilities, and service levels between Proact and The Customer.

4.1 - Modern Workspace Service Operations Standard Operations

Within the context of this Managed Service Agreement, Proact shall provide management of the AVD resources within The Customer's Microsoft Azure Virtual Desktop (AVD) environment that are managed through Nerdio Manager for Enterprise (NME).

The Customer currently has the IaaS services running on-premises utilising Azure Local infrastructure; however, this can be migrated to Azure Public Cloud with no changes to the below scope.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Respond to reasonable service requests for relevant information and advice.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems.
The following elements are out of scope of the service: • Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.

Standing Charge
Proact shall: • Provide the Customer administrator with access to the Proact monitoring portal. • Provide an encrypted tunnel over the internet to secure service traffic. • Provide internet bandwidth for the transfer of service traffic. • Deploy remote monitoring applications to collect statistics/events/alerts for CIs. • Deploy remote management applications to manage CIs.

- Create monitoring profiles to meet the Customer's threshold requirements.
- Provide critical fault alert, vendor co-ordination, incident support and hardware break-fix.
- Provide a service review report.
- Provide a change advisory board to review normal, standard, and emergency change requests.
- Subject to agreement, join the Customer's change advisory board, for relevant changes.
- Implement agreed changes to CIs.
- Provide a major incident report, where required.
- Provide incident trend analysis.
- Organise a quarterly service review meeting.
- Perform pre-planned DR/redundancy tests for CIs during normal Proact business hours.
- Escalate incident alerts to its technical teams for investigation and resolution.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Provide a network administrator to configure and troubleshoot service traffic.
- Provide service accounts and passwords/keys with privileges to allow Proact to manage/monitor the CIs.
- Ensure CIs retain historic log data and make log data available to Proact for troubleshooting.
- Provide sufficient licenses for the CIs to achieve the level of functionality the Customer requires.
- For hardware CIs, provide a minimum of a break-fix vendor support contract.
- For compatible devices, configure 'dial home' diagnostics to report to Proact's service desk.
- Provide 'on demand' remote access to managed CIs, when required by Proact.
- Provide and manage servers/cloud instances to host the remote monitoring/management applications.
- Install CI software major version upgrades to introduce functionality or remain in vendor support.
- Inform Proact of planned maintenance or other operations that may impact the service.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Nominate named individuals to engage with Proact on the approval and timing of changes.
- Work with Proact to agree predefined actions for common types of incidents.
- Provide thirty day's notice of the intention to perform a DR/redundancy test for CIs.
- Provide Proact with a DR/redundancy test plan for all CIs seven working days prior to testing.

The following elements are out of scope of the service:

- DR/redundancy testing performed outside of local business hours.

Virtual Apps and Desktops

Proact shall:

- Monitor/manage the configuration, policies and settings of the Modern Workspace Environment (MWE).
- Work with the Customer to manage public cloud access roles, identities and multi-factor authentication.
- Limit access to the public cloud tenant through limited public IP address ranges.
- Monitor/manage the CIs within the MWE.
- Monitor resource health status, availability, identity, and access management alerts.
- Create deploy and update code for streamline and automate management of the MWE.
- Monitor/Manager cloud service native key vaults, where related to the MWE.
- Monitor/Manager cloud service native databases and log tools, where related to the MWE.
- Monitor/Manager cloud service native storage and automation tools, where related to the MWE.
- Monitor/Manager cloud service native virtual networks, and network security tools, where related to the MWE.
- Perform user density and load balancing checks to ensure optimal performance
- Suspend user sessions and user profiles, where required.
- Inform the Customer of maintenance activities impacting the MWE.

The Customer shall:

- Provide access to the public cloud tenant and network.
- Provide Proact with access to the Modern Workspace Environment (MWE) for Proact to Manage.
- Utilise the public cloud providers native identity and access management tooling.

• Work with Proact to manage public cloud access roles, identities and multi-factor authentication. • Limit access to the public cloud tenant through limited public IP address ranges.. • Maintain overall responsibility security posture, policies and settings of the public cloud tenant and MWE. • Provide access to required native, and third-party, access keys stored within the public cloud key vault. • Inform Proact of changes that may impact security of the cloud platform. • Inform Proact of user sessions or user profiles to be suspended. • Manage file & directory permissions within file shares. • Monitor/Manage, configure and ensure MWE compatibility for end user devices and peripherals. • Manage and troubleshoot end user device hardware and network access to the MWE.
The following elements are out of scope of the service: • Expansion of the MWE into additional public cloud regions or environments. • Upgrades or enabling of new features within the public cloud tenant or virtual desktop environment.

Master Image
Proact shall: • Work with the Customer to deploy and update master images. • Update endpoint master images with patches/security updates and roll out to endpoint devices. • Change MWE policies when requested, or when recommended by the vendor. • Deploy host pools based upon the master images. • Report on host pool resources which reach Customer defined size thresholds. • Assign host pools to required user groups. • Perform master image optimisations or scaling policy changes to improve performance and scale. • Deploy, update or remove Common Applications within master images. • Work with the Customer to deploy, update or remove Uncommon Applications within master images. • Make cost recommendations related to modern workspace environment during quarterly service review.
The Customer shall: • Define the schedule for updating master images. • Provide a valid public cloud, public cloud virtual desktop and MS Windows10/11 enterprise subscription. • Define the usage and application requirements for master images. • Define size thresholds for host pool resources. • Inform and work with Proact to deploy, update or remove Common and Uncommon Applications. • Provide software package, instructions, and user rights needed to update Uncommon Applications. • Provide valid licenses/subscriptions for all Common Applications and Uncommon Applications. • Define: Test, Acceptance, and Production user groups for staged application deployment. • Provide Proact with non-privileged accounts that mimic production users for testing, where required. • Validate Common and Uncommon Application deployment success and functionality.
The following elements are out of scope of the service: • Creation of new master images.

4.2 - Service Level Agreement

4.2.1 - Response Time Service Levels

Definition	Description
Response	Proact is deemed to have ‘responded’ when a case is created in Proact’s customer support portal and a case number is allocated.

Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: • a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or • an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or • an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges for the directly affected service.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges for the directly affected service.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised.

	A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

4.3 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

Vendor Name
LogicMonitor

4.4 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract. The CIs will be the relevant Virtual Desktop Users and Master Images within the Customer's public cloud virtual desktop environment managed by Proact, as set out in the Contract.
Modern Workspace Environment (MWE)	The Customer's public cloud virtual desktop environment. This environment runs pools of virtual desktops, allowing the Customer's users to connect to these desktops to access their business applications.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Common Applications	Are a set of business applications common to the majority of master images. The following applications are defined as Common Applications: Microsoft Windows Microsoft Azure Virtual Desktop Agent (VDA) Microsoft Edge Adobe Reader Microsoft Office
Uncommon Applications	Any application the customer wishes to install within their master images not explicitly listed within the 'Common Applications' definition above.

Appendix 5 - Service Operations for Modern Workspace – Citrix

Proact shall provide management of the Citrix Cloud deployment & Citrix NetScaler (ADC) platform deployed within the Customer's on-premise datacentre. The scope includes operational monitoring, configuration management, optimisation, and lifecycle support for all Citrix Cloud and NetScaler components. This service definition outlines the scope, deliverables, responsibilities, and service levels between Proact and The Customer.

5.1 - Workspace Premium Operations

Within the context of this Managed Service Agreement, Proact shall provide management of the Citrix Cloud deployment hosted on premise.

5.1.1 - General Service Deliverables

Proact Shall:

- Provide a service desk and customer support portal to report and update incidents, change requests and escalations.
- Provide a Service Platform.
- Provide service delivery management.
- Maintain documentation of the service configuration.
- Maintain a CMDB listing for all CIs.
- Respond to Service Platform alerts and events and notify the Customer of relevant incidents.
- Coordinate any product vendor involvement necessary.
- Take appropriate action to restore operation of the Service Platform in case of outage.
- Respond to reasonable service requests for relevant information and advice.

The Customer shall:

- Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level.
- Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone.
- Assist with any systems or applications not under Proact's management.
- Respond to requests for information/actions within five working days. Inactive incidents may be closed.
- Resolve health issues on customer-managed systems.

The following elements are out of scope of the service:

- Upgrades or enabling of new features on the Service Platform. Proact may upgrade the platform at its sole discretion.
- Requests for new business systems, regions, updates, or Azure features require a separately chargeable Proact Professional Services engagement for design, planning, and implementation.

5.1.2 - Standing Charge

Proact Shall:

- Provide the Customer administrator with access to the Proact monitoring portal.
- Provide an encrypted tunnel over the internet to secure service traffic.
- Provide internet bandwidth for the transfer of service traffic.
- Deploy remote monitoring applications to collect statistics/events/alerts for CIs.
- Deploy remote management applications to manage CIs.
- Create monitoring profiles to meet the Customer's threshold requirements.
- Provide critical fault alert, vendor co-ordination, incident support and hardware break-fix.
- Provide a service review report.
- Provide a change advisory board to review normal, standard, and emergency change requests.
- Subject to agreement, join the Customer's change advisory board, for relevant changes.
- Implement agreed changes to CIs.
- Provide a major incident report, where required.
- Provide incident trend analysis.
- Organise a quarterly service review meeting.
- Perform pre-planned DR/redundancy tests for CIs during normal Proact business hours.
- Escalate incident alerts to its technical teams for investigation and resolution.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.

- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Provide a network administrator to configure and troubleshoot service traffic.
- Provide service accounts and passwords/keys with privileges to allow Proact to manage/monitor the CIs.
- Ensure CIs retain historic log data and make log data available to Proact for troubleshooting.
- Provide sufficient licenses for the CIs to achieve the level of functionality the Customer requires.
- For hardware CIs, provide a minimum of a break-fix vendor support contract.
- For compatible devices, configure 'dial home' diagnostics to report to Proact's service desk.
- Provide 'on demand' remote access to managed CIs, when required by Proact.
- Provide and manage servers/cloud instances to host the remote monitoring/management applications.
- Install CI software major version upgrades to introduce functionality or remain in vendor support.
- Inform Proact of planned maintenance or other operations that may impact the service.
- Be billed directly by the cloud provider for any public cloud resources consumed.
- Nominate named individuals to engage with Proact on the approval and timing of changes.
- Work with Proact to agree predefined actions for common types of incidents.
- Provide thirty day's notice of the intention to perform a DR/redundancy test for CIs.
- Provide Proact with a DR/redundancy test plan for all CIs seven working days prior to testing.

The following elements are out of scope of the service:

- DR/redundancy testing performed outside of local business hours.

5.1.3 - Citrix Cloud

Proact Shall:

- Monitor and Maintain Platform Health
  Continuously monitor the health status and operational availability of Citrix Cloud services, including Machine Catalogs, Delivery Groups, and associated file shares.
  Track logon performance, utilisation, and resource health to proactively identify issues.
- Performance and Capacity Management
  Perform user density and load balancing checks to ensure optimal performance.
  Adjust VDA resources where applicable to optimise the environment, including:
  Scale Out/In and Scale Up/Down hosts
  VM placement optimisation
  Storage configuration tuning
  MCSIO configuration adjustments
- Operational Reviews and Best Practice
  Conduct quarterly reviews of the Citrix platform for best practice recommendations and performance tuning.
  Inform the Customer of any maintenance activities impacting the Citrix Cloud platform.
- Session and Profile Management
  Reset suspended user sessions reported by the Customer.
  Remove inactive user profiles as identified by the Customer.
  Manage Microsoft FSLogix profiles used within the Citrix environment.
- Configuration and Change Management
  Manage Citrix Cloud configuration items:
  Active Directory (Identity & Authentication)
  User Profile Management
  Machine Creation Services
  Citrix Director and Citrix Studio
  Implement policy changes as requested by the Customer or advised by vendor support.
  Manage storage and network changes specific to Citrix target devices and associated profiles.
  Manage identity and authentication configuration changes, including conditional access and MFA.
  Develop and maintain all automation code centrally in Proact's DevOps environment for consistency, reuse, and change control.

The Customer shall:

- Provide information on inactive user profiles.
- Perform acceptance testing of changes made to the Citrix Cloud environment.
- Manage file/directory-level permissions via ACLs within file shares.
- Provide Proact with sufficient access to Citrix Cloud and on-premises infrastructure.
- Manage and configure end-user devices and peripherals for compatibility.
- Maintain all other network connectivity between end-user devices, Citrix VDAs, and backend services.
- Define and manage Azure Entra conditional access and MFA policies.
- Maintain valid Microsoft 365 or Windows Enterprise subscriptions and Citrix licensing throughout the contract term.

Jointly, Proact and The Customer shall:

- Work with application vendors for integration and troubleshooting.

- Enable management access via LogicMonitor using Proact's supplied ARM template and parameters file.
- Secure all sign-in activity to Citrix Cloud with conditional access and MFA or verified IP ranges.
- Define customised monitoring thresholds using Proact's standard monitoring toolset.

5.1.4 - Master Image

Proact Shall:

- Work with the Customer to deploy and update master images.
- Update endpoint master images with patches/security updates and roll out to endpoint devices.
- Deploy host pools based upon the master images.
- Report on host pool resources which reach Customer defined size thresholds.
- Assign host pools to required user groups.
- Perform master image optimisations to improve performance and scale.
- Deploy, update or remove Common Applications within master images.
- Work with the Customer to deploy, update or remove Uncommon Applications within master images.

The Customer shall:

- Define the schedule for updating master images.
- Define the usage and application requirements for master images.
- Define size thresholds for host pool resources.
- Inform and work with Proact to deploy, update or remove Common and Uncommon Applications.
- Provide software package, instructions, and user rights needed to update Uncommon Applications.
- Provide valid licenses/subscriptions for all Common Applications and Uncommon Applications.
- Define: Test, Acceptance, and Production user groups for staged application deployment.
- Provide Proact with non-privileged accounts that mimic production users for testing, where required.
- Validate Common and Uncommon Application deployment success and functionality.

The following elements are out of scope of the service:

- Creation of new master images.

5.1.5 - Citrix NetScaler ADC

Proact Shall:

- Monitor and Maintain NetScaler Health
  Continuously monitor the health status and operational availability of all NetScaler appliances and associated services.
  Track SSL offload performance, load balancing metrics, and gateway session health.
  Proactively identify and remediate issues impacting connectivity or performance.
- Configuration and Policy Management
  Manage and maintain NetScaler configuration items, including:
  - Load Balancing Virtual Servers
  - Gateway Virtual Servers
  - Authentication and Authorisation policies
  - SSL certificates and key management
  - Traffic policies and responder policies

  Implement configuration changes requested by the Customer or recommended by vendor best practices.
- Security and Compliance
  Maintain SSL/TLS configurations to align with current security standards.
  Apply updates and patches to mitigate vulnerabilities.
  Configure and manage MFA and conditional access policies for secure remote access.
  Monitor and enforce security policies for ICA proxy and VPN access.
- Performance Optimisation
  Review and optimise load balancing algorithms and persistence settings.
  Tune NetScaler Gateway for optimal HDX performance.
  Conduct quarterly performance reviews and provide best practice recommendations.
- Certificate Lifecycle Management
  Monitor certificate expiry and notify the Customer in advance.
  Install and update SSL certificates provided by the Customer.
  Validate certificate chains and ensure proper binding to virtual servers.
- Firmware and Update Management
  Schedule and implement firmware upgrades in line with vendor recommendations.
  Validate post-upgrade functionality and rollback if required.

- Logging and Analytics
  Configure and maintain NetScaler logging and auditing.
  Provide visibility into traffic patterns and security events.
  Integrate with Customer SIEM or monitoring platforms where applicable.

The Customer shall:

- Provide SSL certificates and associated private keys for installation.
- Define authentication requirements and MFA policies.
- Maintain DNS records and IP address allocations for NetScaler services.
- Provide Proact with sufficient access to NetScaler appliances and management interfaces.
- Perform acceptance testing of configuration changes and upgrades.
- Ensure network connectivity between NetScaler appliances and backend services.
- Maintain licensing for Citrix ADC appliances and any advanced features (e.g., Gateway, GSLB).

Jointly, Proact and The Customer shall:

- Collaborate on design and implementation of new virtual servers or policies.
- Coordinate maintenance windows for firmware upgrades and major changes.
- Define customised monitoring thresholds using Proact's standard monitoring toolset.
- Secure management access via conditional access and MFA or verified IP ranges.

5.2 - Service Level Agreement

5.2.1 - Response Time Service Levels

Definition	Description
Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes. A P1 incident is: • a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or • an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or • an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges for the directly affected service.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is

	significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges for the directly affected service.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is: • a reasonable request by the Customer for support or information; or • an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours of the change being agreed. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.

Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

5.3 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/.

- Legal, Compliance and Privacy Information - Citrix

5.4 - Glossary

Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract. The CIs will be the relevant Azure and/or Nerdio resources for use by the AVD general operation set out in the Contract.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.
Common Applications	Are a set of business applications common to the majority of master images. The following applications are defined as Common Applications: Microsoft Windows Microsoft Azure Virtual Desktop Agent (VDA) Microsoft Edge Adobe Reader Microsoft Office
Uncommon Applications	Any application the customer wishes to install within their master images not explicitly listed within the 'Common Applications' definition above.