[Customer Name]

&

METCLOUD Limited

SERVICES SCHEDULE

Version: 5

Classification: Commercial in Confidence

Change Log			
Description of Change:	**Change Made By:**	**Date of Change:**	**New Document Version:**

Contents

1 Summary

This document serves the purpose of 'Schedule of Services' and is to be referred to in tandem to the overarching contract between [The Customer] and METCLOUD Limited [The Contractor].

The schedule of services provides definitions for services provided to The Customer by The Contractor and includes details of any service level agreements and KPIs.

The services defined throughout this document have been listed below for ease of reference. There are services defined which may not currently feature within your Financial Schedule but included in the event that the services are required in future.

HOSTED SERVICES

Infrastructure as a Service (IaaS)
Disaster Recovery as a Service (DRaaS)
Backup as a Service (BaaS)
Security Operations Centre as a Service (SOCaaS)

MANAGED SERVICES

Service Desk
IT Operations
Security
Account Management
Contract Management
Billing
Licencing
Documentation
Asset Management

2 Hosted Services

2.1 Infrastructure as a Service (IaaS)

2.1.1 Description of Service:

The Contractor's IaaS platform delivers compute and storage as virtual machines via a contractors managed virtualisation layer. The Contractor will manage the underlying IT infrastructure which includes all storage, server, networking and will ensure that the platform is kept up to date and in line with The Contractor's IT security processes.

2.1.2 Service Provision

The Contractor will:

a. provide The Customer with compute and storage as virtual machines via a managed virtualisation layer
b. support and maintain the underlying IT infrastructure of the platform which includes all storage, server, and networking, this includes the application of updates and patches ensuring that the security of the platform is always considered.
c. provide The Customer with a 'service desk', accessible via telephone and email with queries, problems or incidents relating to the platform. If The Customer also subscribes to The Contractors managed service desk, please refer to the ITIL aligned policies and procedures detailed in the related section.
d. provide specific reporting, in a format agreed with The Customer, covering The Customer's systems, performance, and resource utilisation.
e. provide advisory services enabling The Customer to take advantage of increased efficiency, reduced costs, and improvements in service.

2.1.3 Scheduled Maintenance

a. Scheduled maintenance of The Contractor's hosted platform does not in normal circumstances require system downtime.
b. Where downtime is required, service shall not be guaranteed, and all SLAs are suspended during this period. Where downtime is required, The Contractor will endeavour to carry out this activity between 23.00 local time and 07.00 local time (GMT or BST as applicable), Monday through to Sunday, but reserve the right to carry out maintenance outside of these hours should it be necessary.
c. All scheduled maintenance work will be notified to The Customer via e-mail detailing work to be carried out and the possible impact to The Customers Services. Such notifications

will be given at least 48 hours prior to the maintenance being carried out and The Contractor will endeavour, wherever practical, not to schedule maintenance work more than once per week.

d. Where, in The Contractor's reasonable opinion, an emergency exists, The Contractor also reserves the right to carry out emergency maintenance outside this period and without the normal notification process.

2.1.4 Service Level Agreement

Please see section **2.4 Hosted Service – Service Level Agreement**

2.2 Backup as a Service (BaaS)

2.2.1 Description of the Service.

The Contractor will provide Backup as a Service (BaaS) for servers hosted on the IaaS platform, email data from Office 365 and, as required, devices on The Customer's premises.

The BaaS solution will offer:

- Instant Single/Multi Server Recovery for all servers hosted on The Contractors IaaS platform
- Ransomware Protection
- Flexible Data Retention
- Data Encryption

2.2.2 Service Provision

The Contractor will:

a. provide The Customer with a stable backup platform to protect The Customer's data.
b. ensure that The Customer's backup data is protected from unauthorised physical access in line with Tier 3 datacentre standards as defined by the uptime institute.
c. ensure that The Customer's backup data is encrypted and isolated to protect from unauthorised digital access. Software utilised in this service is provided by and subject to third party terms & conditions.
d. support and maintain the underlying IT infrastructure of the platform which includes all storage, server, and networking.
e. To support tenants of the platform with a 'service desk', accessible via telephone and email with queries, problems or incidents relating to the platform. If The Customer also

subscribes to The Contractor's managed service desk, please refer to the ITIL aligned policies and procedures detailed in the related section.

f. To provide (where required) specific reporting and evidence in relation to The Customer systems, performance, and consumption.
g. To provide advisory services enabling The Customer to take advantage of increased efficiency, reduced costs, and improvements in service.

2.2.3 Scheduled Maintenance

a. Scheduled maintenance of The Contractor's hosted platform does not in normal circumstances require system downtime.
b. Where downtime is required, service shall not be guaranteed, and all SLAs are suspended during this period. Where downtime is required, The Contractor will endeavour to carry out this activity between 23.00 local time and 07.00 local time (GMT or BST as applicable), Monday through to Sunday, but reserve the right to carry out maintenance outside of these hours should it be necessary.
c. All scheduled maintenance work will be notified to The Customer via e-mail detailing work to be carried out and the possible impact to The Customers Services. Such notifications will be given at least 48 hours prior to the maintenance being carried out and The Contractor will endeavour, wherever practical, not to schedule maintenance work more than once per week.
d. Where, in The Contractor's reasonable opinion, an emergency exists, The Contractor also reserves the right to carry out emergency maintenance outside this period and without the normal notification process.

2.2.4 Service Level Agreement

Please see section **2.4 Hosted Service – Service Level Agreement**

2.3 Disaster Recovery as a Service (DRaaS)

2.3.1 Description of the Service.

The Contractor will provide Disaster Recovery as a Service (DRaaS) tailored exclusively for servers hosted on the IaaS platform. This comprehensive service ensures robust data, application, and infrastructure recovery in the face of unexpected disruptions.

The DRaaS solution will offer:

- Server Recovery for servers hosted on the Contractor's IaaS platform.
- Flexible replication configurations
- Data Encryption

2.3.2 Service Provision

The Contractor will:

a. Provide The Customer with a stable disaster recovery platform to ensure rapid and reliable recovery of critical data hosted on the IaaS platform.
b. Implement measures in line with Tier 3 datacenter standards to safeguard disaster recovery data from unauthorised physical access.
c. Employ encryption and isolation techniques to safeguard disaster recovery data from unauthorised digital access, utilising third-party software with associated terms & conditions.
d. Support and maintain the underlying IT infrastructure, covering storage, server, and networking components dedicated to disaster recovery.
e. Offer a responsive 'service desk' accessible via telephone and email, addressing queries, problems, or incidents related to disaster recovery.
f. Provide specific reporting and evidence related to The Customer's disaster recovery systems, performance, and consumption, as needed.
g. Provide advisory services to empower The Customer with increased efficiency, reduced costs, and improvements in disaster recovery service.

2.3.3 Scheduled Maintenance

e. Scheduled maintenance of The Contractor's hosted platform does not in normal circumstances require system downtime.

f. Where downtime is required, service shall not be guaranteed, and all SLAs are suspended during this period. Where downtime is required, The Contractor will endeavour to carry out this activity between 23.00 local time and 07.00 local time (GMT or BST as applicable), Monday through to Sunday, but reserve the right to carry out maintenance outside of these hours should it be necessary.

g. All scheduled maintenance work will be notified to The Customer via e-mail detailing work to be carried out and the possible impact to The Customers Services. Such notifications will be given at least 48 hours prior to the maintenance being carried out and The Contractor will endeavour, wherever practical, not to schedule maintenance work more than once per week.

h. Where, in The Contractor's reasonable opinion, an emergency exists, The Contractor also reserves the right to carry out emergency maintenance outside this period and without the normal notification process.

2.3.4 Service Level Agreement

Please see section **2.4 Hosted Service – Service Level Agreement**

2.4 Security Operations Centre as-a-Service (SOCaaS)

2.4.1 Description of the Service

The Contractor will provide a Security Operations Centre as-a-Service (SOCaaS) platform providing a fully managed SIEM (Security Information and Event Management) and SOC (Security Operations Centre).

SIEM (Security Information and Event Management):

The SIEM will aggregate and analyse activity from across The Customer's entire IT infrastructure, stores, normalizes, aggregates, and applies analytics to that data to discover trends and detect threats,

SOC (Security Operations Centre):

The SOC will on a 24-7 basis review, investigate, and resolve alerts generated by the SIEM system. Where service desk functions are included within the subscribed services, the SOC is integrated into The Contractor's service desk to provide that end-to-end resolution of potential security threats. In addition to this, monthly security reports and reviews are conducted by a dedicated cyber security account manager. Whereby the SOC is not integrated into The Contractors' service desk, an alternate customer contact will be defined.

2.4.2 Service Provision

The Contractor will:

a. provide a 'management/storage head' server with the agreed compute resources.
b. configure the 'management/storage head' server.
c. provide the 'collector' software and configuration guidance for the client.
d. Provide 365 business days' log retention within the SIEM solution.
e. configure log feeds for the devices to be monitored by the SIEM solution.
f. ensure all alerts and incidents are investigated to conclusion.
g. ensure all reasonable service requests are managed to completion. Where a service request is deemed out of scope, The Contractor will provide a quote for the requested services.
h. provide a monthly report summarising SIEM and SOC activities and highlight any potential areas for improvement or for concern.
i. facilitate a monthly meeting to review the ongoing service and report.
j. provide (where required by The Customer) specific reporting and evidence in relation to The Customer's systems, performance, and consumption.
k. provide advisory services enabling The Customer to take advantage of increased efficiency, reduced costs, and improvements in service.

2.4.3 Scheduled Maintenance

a. Scheduled maintenance of The Contractor's hosted platform does not in normal circumstances require system downtime.
b. Where downtime is required, service shall not be guaranteed, and all SLAs are suspended during this period. Where downtime is required, The Contractor will endeavour to carry out this activity between 23.00 local time and 07.00 local time (GMT or BST as applicable), Monday through to Sunday, but reserve the right to carry out maintenance outside of these hours should it be necessary.
c. All scheduled maintenance work will be notified to The Customer via e-mail detailing work to be carried out and the possible impact to The Customers Services. Such notifications will be given at least 48 hours prior to the maintenance being carried out and The Contractor will endeavour, wherever practical, not to schedule maintenance work more than once per week.
d. Where, in The Contractor's reasonable opinion, an emergency exists, The Contractor also reserves the right to carry out emergency maintenance outside this period and without the normal notification process.

2.4.4 Service Level Agreement

Please see section **2.4 Hosted Service – Service Level Agreement**

2.5 Hosted Services - Service Level Agreement

2.5.1 Support Response Definitions

The Contractor will provide hosted Services to ensure 99.9% uptime measured over a 90-day period. Only a systems failure known to The Contractor which emanates from the hardware and hypervisor layers delivering the Cloud Platform service will constitute a failure and be covered by this SLA, subject to the following exclusions:

- Power Interruptions beyond the control of The Contractor
- Catastrophic event outside of the control of The Contractor rendering the Data Centre inoperable.
- Denial of Service attack targeting the Data Centre infrastructure.
- Zero Day vulnerabilities.
- A flaw introduced in third-party code that affects the stability of The Contractor's hosted platform.

2.5.2 Support Response Definitions

Each support category and their expected response times are based on Priority Levels defined as follows:

Priority 1:

Priority 1 is an error isolated to the METCLOUD aaS (as-a-Service) infrastructure that renders the service inoperative or causes the service to fail catastrophically i.e., major system impact or system outage. This issue must be resolved before The Customer can use the service. All Priority 1 issues have no workaround, and The Contractor and Customer shall work closely together to resolve the error as soon as possible.

Priority 2:

Priority 2 is an error isolated to the METCLOUD aaS Infrastructure and Multi-Tenant services which causes a serious impairment to a critical feature of the Service, but where overall functionality is not interrupted. Usually, a workaround is available for this type of issue, but such is not always the case.

Priority 3:

Priority 3 is an issue that causes the failure of a non-critical aspect of the infrastructure and multi-Tenant service and a satisfactory work-around already exists, but the presence of this issue will result in customer dissatisfaction.

Priority 4:

Priority 4 is an issue of minor significance which results in a slight variance between the services provided and the service specified.

2.5.3 METCLOUD Platform Service Interruption Priority Levels

A service failure will be categorised as follows:

METCLOUD Platform Service Interruption Priority Levels	Response Type	Notification Response from Start of Incident	Subsequent Responses until Resolution
Priority 1	Initial contact followed by System Status communications	Within 15 minutes	Update each 30 minutes via pre-agreed communication method
Priority 2	Initial contact followed by System Status communications	Within 30 minutes	Update each 60 minutes via pre-agreed communication method
Priority 3	Initial contact followed by System Status communications	Within 60 minutes	Update each 120 minutes via pre-agreed communication method
Priority 4	Initial contact followed by System Status communications	Within 120 minutes	Update each 180 minutes via pre-agreed communication method

2.5.4 Response Schedule for Service Interruptions

a. For Priority 1 and 2 issues a root cause analysis response will be provided within 14 days from the successful resolution of the incident.
b. The Contractor will continually monitor all hosted services, refer to section **2.4.1, 2.4.2 and 2.4.3 for SLA Details.**
c. The Contractor will inform The Customer as soon as practicable (via pre-agreed communication method).
d. Should The Customer suspect performance or availability issues then, The Customer must report it promptly to The Contractor via pre-agreed communication method. The fault will be logged within the ticketing system from that point and relevant action taken in accordance with the terms set out in the agreement and this SLA.

	Response Procedures	Time
A	Establish Priority and impact of the outage	Within 15 minutes
B	Troubleshoot and take necessary steps to resolve the problem. Where fault is at the application layer, notify Customer immediately. Where available, instigate applicable failover systems following agreed protocols (see below)	Within 30 minutes
C	If outage is due to a major hardware failure, then it may be required to replace the faulty component.	Within 8 hours
D	Record fault and verify resolution of the outage	Within 24 Hours

2.5.5 SOCaaS Service Level Agreement

Security Monitoring Severity Definitions

Severity	Description
P1 / High	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a PROBABLE (current, possible impact) threat against business impacting customer assets.
P2 / Medium	An Incident identified either by automated correlation rules or through SOC analysis that is deemed to be a POTENTIAL (not current, may have future impact) threat against business impacting customer assets.
P3 / Low	An Incident identified either by automated correlation rules or through SOC analysis that may require further investigation, with no apparent threat against business impacting customer assets.

Security Monitoring Detection SLA

Severity	Detection Time
P1 / High	1 Hour
P2 / Medium	3 Hours
P3 / Low	6 Hours

Security Remediation SLA

If The Customer has an active managed support contract, then remediation of detected incidents will align with the incident Management SLAs defined in section **3.1.4 Incident Management – Service Level Agreements.**

2.5.6 Service Credits

In the event that The Contractor's hosted platform uptime of 99.9% is not reached, the Contactor shall pay to The Customer the following service credits:

Availability of Network in a 90-day period	Service Credit
Less than 99.9%	Quarterly hosted services value/2160 hours x actual downtime = Service Credit.

2.5.7 Customer Managed Systems

Customer Managed Systems are defined as any systems which are managed by a customer or their sub-contractor.

In the event of a failure of The Customer Managed System, The Contractor will work with The Customer and use all commercially reasonable endeavours to return the systems to a pre-failure state:

a. The Contractor will use sole discretion to determine the extent to which any effort, assistance and/or support resources are utilised to recover The Customer's systems and any associated data.
b. No warranties will be given or provided for any Customer recovery of systems.

2.5.8 General Exclusions and Limitations

Notification: The Customer must notify The Contractor within sixty (60) business days from the time The Customer becomes eligible to receive a credit as set out in the SLA to receive such credit. Failure to comply with this requirement will forfeit The Customer's right to receive a credit.

Service Credit Limitations: For the avoidance of doubt, The Contractor shall not be liable to pay any more to The Customer by way of service credits in any ninety-day period than a sum which is equal to the VAT exclusive amount of 50 % of the monthly recurring service charges regardless of the number of incidents or failures in that quarter.

Acceptable Use Policy: If customer is in breach of the 'Acceptable Use Policy' and this causes a service failure, this shall not be deemed to be a failure of The Contractor to provide services in accordance with the service levels set out in this SLA and therefore service failures which occur as a result shall not be considered in computing availability under the service level.

Application of Service Credits: Service Credits apply individually for any one independent event (or series of related events) and shall not accrue concurrently, sequentially or in aggregate as a consequence of the same event (or series of related events) across all service level categories. In this situation, the highest service credit (by amount) will apply.

3 Managed Services

3.1 Service Desk – Description of Service

The Contractor will provide facilities, associated technologies, and appropriately trained staff to respond to calls to the Service Desk from The Customer, facilitate all Incident Management, Problem Management, Change and Request Management activities, and act as a single point of contact for coordination and communication to Authorised Users and third-party Service Providers regarding the Services.

The service desk service underpins all managed services provided by The Contractor (e.g., Server Support, Backup Management etc.). Where products such as mail or web filters are in use, the service desk also provides support for these services in line with the vendor or as agreed during service discussions. A list of all services supported under the service desk operation can be found within the Financial Schedule. Service Desk falls into the following categories which are described in more detail in the following sections:

Managed Service Requests and Incidents: Provide timely and effective response to user and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate, and resolve incidents.
Managed Problems: Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.
Managed IT Changes: Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications, and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure, and documentation.

Note Regarding Third Party Suppliers in relation to all ticket types and related SLAs

- Where agreed 3rd Party Suppliers are not adequately responding to communications, or are failing to meet their service levels, within an agreed Underpinning Contract (UPC), then the Service Desk should capture this information and escalate directly to Customer as this may impact overall SLA attainment.
- For those tickets that are assigned to other customer 3rd Party Suppliers where no UPC is in place we will place these tickets “on hold”. The Contractor will still however try to progress the tickets with the respective 3rd Party suppliers and escalated to The Customer if appropriate via the Service Management escalation processes and policies.

3.1.1 Incident Management

An incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service, or a failure of a configuration item that has not yet impacted IT service. (Example failure of one of the discs in RAID configuration that will not affect the service but increase risk of disaster, and so it becomes an incident) Incident Management aims facilitate the restoration of normal operational service where a failure has occurred as quickly as possible to minimise the adverse impact on business operations. If not set otherwise, every ticket must be treated initially as an incident – to the point it is defined that it is not an incident.

Deliverables

The Contractor will:

a. Provide a single point of contact for the receipt of service incidents, concerns, and queries during the agreed contracted hours.
b. Ensure all incidents are entered into The Contractors' ticket logging system.
c. Follow Incident management processes aligned with the ITIL framework.
d. Co-ordinate with other customer 3rd Party Suppliers involved in the provision of incident management support to encourage ownership of incidents through to resolution. This will involve chasing suppliers, if necessary, to ensure that The Contractor incident records are up to date.
e. Work with The Customer to identify and understand the possible causes and trends of incident types. Any incident trends identified will result in a Problem Record being raised and assigned for Problem Management to then manage.

3.1.2 Major Incident Management

A P1 incident is treated as a **Major** incident when it stops a significant number of users from carrying out daily work, resulting in increased backlog size of business processes that are growing and risking incidents spread. For example, in cloth producing organisation, the failure of the accounting server will result in a P1 incident that stops the process of generating payslips on the due date. Still, it was indicated that it is an isolated case and will not spread incidents, so it is not classed as a major incident.

When a major incident is occurs, the service desk manager automatically becomes the Major Incident Manager (MIM) unless there is a reason for an alternative individual to assume this role. For Information Security Major Incident – The Contractor's Information Security Officer becomes MIM.

The Major Incident Management ensures that the management and resolution of this ticket receives dedicated co-ordination and provides the Major Incident Manager with access to additional resources to achieve a resolution.

3.1.3 Incident Management – Prioritisation

Incident impact Levels are directly correlated to the priority which will assigned to the incident. Prioritisation of tickets is based on Risk and Backlog to ensure the process is versatile to adapt to all types of incidents.

Priority	Criteria/conditions
Critical - P1	• downtime on The Customer's business-critical (core) systems • incidents that stop a significant number of users from carrying out daily work that is resulting in increased backlog size of business processes that are not cleaned but not risking in incidents spread • any appeared risk that goes over risk acceptance level that may result in an incident on this level
High – P2	• downtime on The Customer's business-critical (core) systems that lasted for at least a few hours even if it back to its normal state • incidents that prevent significant users from carrying out their daily work that is resulting in increased backlog size of business processes that are slowly cleaned but without decreasing it and is not risking in incidents spread • any appeared risk that goes over risk acceptance level that may result in an incident on this level
Medium – P3	• incidents that prevent or were preventing significant users from carrying out their daily work resulting from or has resulted in increased backlog size of business processes that are slowly cleaned and decreasing it. • downtime on The Customer's business-critical (core) systems that lasted for less than a few hours even if it back to its normal state • any appeared risk that goes over risk acceptance level that may result in an incident on this level • there are no incidents spread risk
Low – P4	• incidents that affect at least one user, where the user is not prevented from carrying out their daily work • there is no business-critical (core) level backlog • there is no risk that incident of higher level will appear

3.1.4 Incident Management – Service Level Agreements

All SLAs are default in cases that are not defined specifically within the contractual arrangement.

Initial response time is the number of minutes or hours passed from the time a customer first submits their case and an agent responds to it. This metric is best measured in business hours, there's no penalty for time off the clock.

Resolution is defined as the provision of a fix, workaround, or acceptance that it is a known error with no current fix and thus resolved against a Problem Record. The incident is not put in a "Resolved State" until confirmation is received.

Service Measures	Service Level Target	KPI measure	Service credits
SLA Response Times P1 – Response within 20 Mins P2 – Response within 90 Mins P3 – Response within 5 Hours P4 – Response within 8 Hours **E-mail response**, Service Desk Mailbox confirmation receipt issued on arrival of end user email, followed by notification & ticket number from Service Management Tool (PSA) once ticket is created from the e-mail. Response time for e mail contacts will be time between email arrival and PSA ticket number notification being generated. SLA Resolution Times P1 – 4 Business hours P2 - 8 Business hours P3 - 3 Business days P4 - 10 Business days ** Major problems are always as P1 Incidents **	95%	Number of Incidents by Priority Number of Incidents per day Number of Incidents by fault type Number of Incidents Resolved Number of Incidents Closed	In Month 1: Nil In Month 2 and each subsequent Default Month: £400

3.1.5 IT Service Requests

Service Requests are requests from a user for information, advice, a standard change, or access to a service.

A standard change is simply a pre-approved change that is low risk and that follows a standard procedure.

Service Requests are managed by the service desk. Examples of such requests include but are not limited to; Requests for information, advice, or the implementation of standard change by users, such as user password change or to provide standard IT Services for a new User.

Deliverables

The Contractor will:

a. Provide a single point of contact for the receipt of customer in-scope of service requests during the agreed contracted hours.
b. Ensure all incidents are entered into The Contractors' ticket logging system.
c. Follow Service Request management processes aligned with the ITIL framework.
d. Co-ordinate with other customer 3rd Party Suppliers involved in the provision of services to encourage ownership of service requests through to fulfilment. This will involve chasing suppliers, if necessary, to ensure that The Contractor records are up to date.

3.1.6 IT Service Requests – Service Level Prioritisation

Service request prioritisation must use a different approach than incident management. There is no current danger to working services and we must consider an emergency, the level of impact and if it will cause any potential risk on changes. Service urgency is related to SLA that may differ depending on contractual arrangements and is used here as default when no other formats are set.

Priority	Criteria/conditions
Critical- P1	• Service request is urgent to be done within 4 business hours, and • client is aware it may require downtime on The Customer's business-critical (core) systems that will stop a significant number of users from carrying out daily work and that may result in increased backlog size of business processes within business hours
High – P2	• service request is urgent to be done within 8 hours, and • client is aware it may require downtime on The Customer's business-critical (core) systems that will stop a significant number of users from carrying out daily work and that may result in increased backlog size of business processes within business hours
Medium – P3	• service request is to be done within 3 business days, and • client is aware it may require downtime on The Customer's business-critical (core) systems outside of business hours, and that may result in increased backlog size of business processes within a business or non-business hours
Low – P4	• service request is to be done within 10 days business days, and • client is aware it may require downtime that will affect at least one user, where the user is not prevented from carrying out their daily work, and there will not be business-critical (core) level downtime or backlog, • there is no business-critical (core) level backlog

Notes

It is also possible that Request fulfilment maybe dependent on the approval and implementation of a Change, therefore the SLA will be aligned with the Change Management SLAs.

3.1.7 IT Service Requests – Service Level Agreement

All SLAs are default in cases that are not defined specifically within the contractual arrangement.

Initial response time is the number of minutes or hours passed from the time a customer first submits their case and an agent responds to it. This metric is best measured in business hours, there's no penalty for time off the clock.

Resolution is defined as the provision of a fix, workaround, or acceptance that it is a known error with no current fix and thus resolved against a Problem Record. The service desk record is not put in a "Resolved State" until confirmation is received.

Service Measures	Service Level Target	KPI measure	Service credits
SLA Response Times P1 – Response within 20 Mins P2 – Response within 90 Mins P3 – Response within 5 Hours P4 – Response within 8 Hours **E-mail response**, Service Desk Mailbox confirmation receipt issued on arrival of end user email, followed by notification & ticket number from Service Management Tool (PSA) once ticket is created from the e-mail. Response time for e mail contacts will be time between email arrival and PSA ticket number notification being generated. SLA Resolution Times P1 – 4 Business hours P2 - 8 Business hours P3 - 3 Business days P4 - 10 Business days	95%	Number of Service Requests raised each month by priority Number of Service Requests resolved each month Number of Service Requests that resulted in a change	In Month 1: Nil In Month 2 and each subsequent Default Month: £400

3.1.8 Problem Management

Problem Management seeks to minimise the adverse impact of Incidents by preventing Incidents from happening. For Incidents that have already occurred, Problem Management tries to prevent these Incidents from happening again. ITIL defines a "Problem" as "the underlying cause of one or more Incidents". Problem Management works closely with Incident Management, but it is not the same:

a. Incident Management is about restoring services as quickly as possible, often by applying temporary solutions.
b. Problem Management is tasked with analysing root causes and preventing Incidents from happening in the future.

All Problems are logged as Problem Records, where their status can be tracked, and a complete historical record maintained. The categorisation and prioritisation of Problems is harmonised with the approach used in Incident Management, to facilitate matching between Incidents and Problems.

The process used for problem management is as follows:

a. Problem Identification
b. Problem Diagnosis
c. Problem Investigation
d. Work Around or Resolution
e. Review / Continuous Improvement

Deliverables

The Contractor will:

a. Facilitate Identification & resolution of recurring or underlying incidents or errors where appropriate.
b. Ensure all problems are entered into The Contractor's ticket logging system.
c. Follow Problem management processes aligned with the ITIL framework.
d. Provide Problem / Root Cause Analysis reports as required within the Problem Management process.
e. Co-ordinate with other customer 3rd Party Suppliers involved in investigation or resolution of problems. This will involve chasing suppliers, if necessary, to ensure that The Contractor records are up to date.

3.1.9 Problem Management – Problem Prioritisation

Priority	Criteria/conditions
Critical- P1	• underlying problem that results in a daily incident • Unknown error with no known workaround
High – P2	• underlying problem that results almost in the daily incident (at least every three working days) • known error registered with a workaround
Medium – P3	• problem that results in weekly incidents or performance issues that do not create an increased backlog • known error registered with a workaround
Low – P4	• problem that results in recurring performance issues that do not create an increased backlog

3.1.10 Problem Management – Service Level Agreement

Service Measures	Service Level Target	KPI measure	Service credits
Supplier to provide Customer with RCA report for (in-scope) P1 incidents within 10 working days of incident resolution. P1 – 10 Days P2 – 30 days P3 – Nil as per any trends found P4 – Nil as per any trends found	95%	Number of Problem records raised during reporting period Number resulting from pro-active incident trend analysis Number of Problem records resulting in a change being raised Number of unresolved Problem records during reporting period	In Month 1: Nil In Month 2 and each subsequent Default Month: £400

3.1.11 Change Management

Change Management seeks to minimise the risk associated with changes. This is achieved by controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved Changes with minimum disruption.

ITIL defines a Change as "the addition, modification of removal of anything that could have an effect on IT services".

This process is typically initiated from a Service Request but can also be initiated because of Incident or Problem Management as well.

Deliverables

The Contractor will:

a. Liaise with The Customer & any of its 3rd Parties to ensure that they use and follow the approved Change Management processes and polices.
b. Ensure all changes are entered into The Contractors' ticket logging system.
c. Follow Change Management processes aligned with the ITIL framework.
d. Facilitate and attend CAB meetings.
e. Co-ordinate with other customer 3rd Party Suppliers involved in the change management process. This will involve chasing suppliers, if necessary, to ensure that The Contractor records are up to date.

3.1.12 Change management: Service Level Agreement

Service Level Target	KPI measure
If change management is invoked through an incident or problem, it will be then part of those items SLA. Change management does not have its SLA as long has not been agreed upon within change or by contractual arrangement.	Number of Changes raised by type Number of changes as result of IMACD (Install, Move, Add, Change, or Decommission) Number of changes implemented successfully Number of changes implemented and backed out Number of unplanned changes identified

3.1.13 Hours of Service

The service desk provides support Mon-Fri 8.00am – 6.00pm excl. Public Holidays.

Exceptions to the hours of service apply for the below services whereby service hours are extended to 7:30pm excl. Public Holidays:

- Major Incident Management (MIM)

3.2 Monitoring

3.2.1 Service Description

The Contractor will provide 24/7 monitoring and reporting on the items specified within the financial schedule. For the avoidance of doubt, items that can be monitored will be denoted by the letter 'M'. The Contractor will respond to events triggered by monitoring during service hours which are Mon-Fri excluding public UK holidays, 08:00hrs to 18:00hrs.

The Contractor will monitor the following for Servers, Storage and Network Devices (As appropriate for each technology):

- CPU performance
- Memory utilisation
- Storage
- Availability
- Hardware Status
- Application Monitoring

For storage, The Contractor will monitor disk utilisation and alert when the used space exceeds the following pre-set thresholds:

- Upon 80% utilisation the monitored storage goes 'amber'
- Upon 90% utilisation the monitored storage goes 'red'
- When the utilisation drops back and below 85% the monitored storage goes 'amber'
- When the utilisation drops back and below 75% the monitored storage goes 'green'

Upon detecting a change in state, The Contractor will log a call on the Service Desk and discuss with The Customer the most appropriate course of action. The Contractor will not delete Customer data unless The Contractor has been advised to do so by The Customer in writing in advance.

The Contractor will monitor and identify areas for fine tuning to provide greater granularity as part of the Support Services at no additional cost to The Customer

Where The Contractor's monitoring has detected a component or system failure, The Contractor will log a ticket on ticketing platform and manage the situation accordingly, The Customer will be made aware of the failure, The Contractor will advise on their course of action to resolve the problem, and they will give regular updates to The Customer on problem resolution.

3.3 Server Support

3.3.1 Service Description

Server support ensures monitoring and management of 'server' computers to maintain a consistently high level of availability, reliability, and security.

The service desk function utilises monitoring and management to deliver this service. The Contractor will monitor the hardware and operating system layer supporting the core Microsoft technologies. Where application (e.g., Endpoint Protection) or role (e.g., Domain Controller) specific monitoring will be provided by The Contractor.

3.3.2 Service Provision – Hardware

The Contractor will:

a. Manage the hardware and ensure it is reliably delivering high availability to The Customer.
b. Install hardware (and replace faulty hardware if there is hardware maintenance in place) and configure using The Contractor's best practice to ensure high systems availability.
c. Advise on systems or configuration improvements, upgrades, or replacement (technology refresh) that will deliver greater systems performance and business benefits.
d. Manage external hardware vendors to repair component or system failures should they occur.
e. Carry out manufacturers updates when advised by the manufacturer or The Customer to either fix a known problem or prevent the occurrence of a problem.
f. Advise The Customer when warranty is due to expire on any part of the System.
g. Attend site should the need arise to assist the manufacturer in problem resolution.
h. Attend site to assist the manufacturer in recovering the system in the event of a system failure.
i. Attend site if a system failure requires an OS and data restore from backups.

3.3.3 Service Provision – Software

The Contractor will:

a. where required as a part of an incident, perform OS installs, upgrades or advise on improvements to maximise the reliability and availability of the windows operating system.
b. undertake server re-boots – where The Customer requests a server to be re-booted, The Contractor will ensure timely delivery of the request, in addition The Contractor will ensure the server has re-booted and returned to service. The Contractor will advise The Customer

once the request has been completed. Requests for re-boots outside of the service hours will be discussed with The Contractor's service delivery or account manager. In certain circumstances a charge may apply for this service, but no additional charges shall be made unless agreed in writing in advance with The Customer.

c. undertake problem solving of specific issues effecting the operation of the server, and where the resolution lies with the manufacturer, escalate, and manage the process.
d. where a specific vulnerability that requires immediate deployment has been identified, The Contractor will action this during the support window. Alternatively, at a cost The Contractor will action the update out-side of the support window, but no additional charges shall be made unless agreed in writing in advance with The Customer.
e. where The Contractor has identified a problem with a specific Windows server, that an update or service packs will resolve, then this is applied, either within the service window, or within an hour after, depending on the specifics of the case, at that time.
f. where The Contractor needs to carry out a server re-boot, for normal support work, The Contractor will endeavour to ensure updates are applied during this process. The Customer will be advised and approve such request to re-boot servers during the service window.
g. Where The Contractor re-builds Windows servers, or install new Windows servers, The Contractor will ensure the server is built with up-to-date service packs and updates, depending on the requirements of the software application.
h. In the event of a system failure, and where a full system recovery is required, The Contractor will assist in the restore of the complete system. Recovery times will depend on the hardware repair, and subject to the availability of current system and data backups.
i. Anti-Virus updates are managed by The Contractor and fall within the scope of Support Services under this Agreement at no additional cost to The Customer.

3.4 Network Support (Firewalls, Switches and Wireless)

3.4.1 Service Description

Network support ensures monitoring and management of 'server' computers to maintain a consistently high level of availability, reliability, and security.

The service desk function utilises monitoring and management functions to deliver this service.

Network support activities include:

a. Remotely access the network device to carry out configuration changes as requested by The Customer.

b. Where required perform OS installs, upgrades or advise on improvements to maximise the reliability and availability of the device's operating system.
c. Problem solving specific issues effecting the operation of the network device, and where the resolution lies with the manufacturer, escalate, and manage the process.
d. Keep documentation for device configurations and hold records of login and password details.
e. Ensure strict adherence to change control policies on critical core enterprise network devices.
f. Attend site to resolve problem as required.
g. Assist the hardware vendor to re-apply an image and configuration should a device require vendor replacement.
h. Manufacturers updates are not automatically carried out by The Contractor. Where the manufacturer advises The Contractor to apply a firmware upgrade to apply a fix to a known problem The Contractor will do so. This work will be carried out under the service contract and during the service window. If The Customer requests this to be done outside of the service window, a charge will apply but no additional charges shall be made unless agreed in writing in advance with The Customer.
i. Where either the manufacturer or The Customer requests manufacturers update to be applied for reasons other than fixing a known problem, The Contractor will treat this as falling outside of the Managed Service, and this will be treated as project work, where the change control procedure will apply, ensuring the appropriate risk assessment is carried out. No additional charges shall be made in this regard unless agreed in writing in advance with The Customer.
j. The Contractor will advise The Customer at least six months before the warranty expires in relation to any part of the System.

3.5 Connectivity

The Contractor does not provide ISP tier connectivity such as internet or MPLS. However, where The Customer provides authorisation to do so and a support agreement is in place with the vendor, The Contractor will assist and facilitate in resolving or responding to incidents, changes, problems by liaising with third party providers.

3.6 Backup Management

3.6.1 Service Description

This service is the process of creating and storing copies of The Customer's data to protect The Customer against data loss. Recovery from a backup typically involves restoring the data to the original location, or to an alternate location where it can be used in place of the lost or damaged data.

A proper backup copy is stored in a separate system or medium, such as cloud storage, from the primary data to protect against the possibility of data loss due to primary hardware or software failure. Backup Monitoring and Management is managed via the service desk function and is in accordance with service desk SLA's.

3.6.2 Service Provision

The Contractor will:

a. check the status of backups in accordance with the backup schedule up to a maximum of once per day.
b. raise the appropriate ticket in the event of a backup failure or issue.
c. investigate and resolve backup issues promptly.
d. report on the backup platform according to the backup scheduled up to a maximum of once per day.
e. ensure The Customer is informed promptly of any potential risks to the integrity of the backup solution or data.
f. provide (where required by The Customer) specific reporting and evidence in relation to The Customer systems, performance, and consumption.
g. provide advisory services enabling The Customer to take advantage of increased efficiency, reduced costs, and improvements in service.
h. Perform ad hoc test restores as requested by The Customer to validate the integrity of backup.

3.7 Disaster Recovery Management

3.7.1 Service Description

Disaster Recovery Management provided by The Contractor minimises downtime and data loss to ensure business continuity, lowers disaster recovery costs, and helps an organisation stay in compliance with regulatory requirements.

The Contractor will monitor and manage the Disaster Recovery Solution in place for The Customer to ensure the greatest opportunity for The Customer to achieve their desired RPO (Recovery point Objectives) and RTO (Recovery Time Objectives).

Recovery Point Objective (RPO). The maximum amount of time that you are willing to lose data on your systems because of an event.

Recovery Time Objective (RTO). How fast you can recover from the moment of a disaster to the moment you return to normal operations.

Refer to The Customers Disaster Recovery plan for details of the solution.

3.7.2 Service Provision

The Contractor will:

a. monitor the status of The Customer's Disaster Recovery solution.
b. raise the appropriate ticket in the event of any issues relating the Disaster Recovery Solution.
c. Where possible, to promptly investigate and resolve issues relating to the Disaster Recovery solution.
d. Where issue resolution is not possible via support, to ensure The Customer is informed of any potential risks and actionable steps are provided to restore the Disaster Recovery Solution as soon as possible.
e. assist The Customer in performing an annual Disaster Recovery test and provide a report in relation to the IT Disaster Recovery in which recommended improvements to the solution are outlined.
f. perform any agreed role designated within the agreed Disaster Recovery process in the event of a disaster situation.
g. provide input and/or update the IT Disaster Recovery process documents held by The Customer.
h. provide (where required) specific reporting and evidence in relation to The Customer systems, performance, and consumption.
i. provide advisory services enabling The Customer to take advantage of increased efficiency, reduced costs, and improvements in service.

4 Managed Security Services

4.1 Cyber Security Advisory

The Cyber Security Advisory service is a service offering where METCLOUD provides direct instruction and guidance to clients based on its organisational knowledge and expertise. This service influences client decisions and outlines the necessary steps to achieve cybersecurity objectives.

4.1.1 Service Provision

The Contractor will provide advice to the Customer for the following areas as a part of an agreed recurring schedule:

a. Cyber security risks
b. Security policies
c. Staff cyber awareness
d. Cyber vulnerabilities
e. Incident response
f. Security architecture
g. Compliance
h. Cyber security roadmap

4.2 Vulnerability Management

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.
The Contractor utilises scanning software to identify and evaluate the security vulnerabilities. Once vulnerabilities have been identified, the evaluation, treatment and reporting of the discovered vulnerability is managed via the service desk using the appropriate ticket type.

4.2.1 Service Provision

The Contractor will:

a. ensure the agreed Customer systems are onboarded onto the vulnerability management platform.
b. review on a weekly basis the vulnerability management platform for the discovery of newly identified vulnerabilities.
c. ensure the appropriate ticketing process is followed for the evaluation and remediation of vulnerabilities.
d. assess and prioritise vulnerabilities based on business and technical impact ensuring the relevant patches and resources are available for treatment of the vulnerability.

e. ensure The Customer is aware of the vulnerabilities highlighted by the vulnerability management platform.
f. where vulnerabilities cannot be treated (technical reason, business reason etc.) the Contact will ensure that The Customer is made aware so the appropriate action can be taken.
g. provide (where required) specific reporting and evidence in relation to The Customer's systems.

4.2.2 Service Level Agreement

Activity	Service Level Target	KPI measure
Identify, Investigate, and provide remediation recommendations for High & Critical Vulnerabilities within 14 days of detection.	95%	Vulnerability Management tickets raised during the reporting period Regular reports to highlight performance against SLA.

Remediation of Vulnerabilities is dependent on multiple variables and cannot be set out as an SLA. Where existing vulnerabilities are inherited or detected following service onboarding, the SLA above does not apply.

4.3 Patch Management

4.3.1 Service Description

Patch Management is the process of managing a network of servers and/or end user devices by regularly performing patch deployment to keep computers up to date. The METCLOUD patch Management service objective is to keep The Customer's systems secure, compliant, up-to-date, and running smoothly.

Patch Management is mainly delivered in an automated fashion by The Contractor's Remote Monitoring and Management tools. A maintenance window(s) is agreed and then configured patch policies run to ensure the installation of patches.

In certain instances (e.g., complex server estate, application etc.) whereby manual intervention is required to ensure the successful installation of patches. In these instances, resource is assigned to maintenance windows to ensure the installation of updates, patches and subsequently the verification of system operation.

By default, the patch management service only includes updates and patching of the core Windows Operating System. If third party patching is added to the service, third party applications (as per supported applications) will also be updated/patched).

4.3.2 Service Provision

The Contractor will:

a. ensure The Customer's agreed systems are onboarded onto the patch management platform where possible.
b. notify The Customer and agree maintenance window(s).
c. install high and critical Microsoft Windows patches and updates made available by the vendor.
d. where Third Party Patch Management is purchased, to install the supported application patches as made available by the vendor.
e. monitor the deployment of updates and patches, ensuring that any issues with the deployment of patches is raised as an appropriate ticket under the service desk function.
f. To provide (where required) specific reporting and evidence in relation to The Customer systems.

5 Account Management

The Contractor will provide The Customer with access to individuals to serve as liaison between the two parties. Their core priority is addressing The Customers' needs and concerns as quickly and effectively as possible to develop and maintain strong relationships.

By means of account management, the below will be delivered by one or multiple individuals from The Contractors' organisation.

5.1 Meetings

a. Monthly Managed Service Review
b. Monthly Information Security Forum Meeting
c. Quarterly Meeting with Account Manager (as agreed)

5.2 Reports

a. Monthly Management Report delivered by the 2nd Wednesday of each month
    - Provides a management level overview of services provided by The Contractor:
        i. Service Desk Summary
        ii. Backup Summary
        iii. Infrastructure Availability
        iv. Storage Consumption
        v. Disaster Recovery
        vi. Security Summary

b. Monthly Security Report delivered by the 2nd Wednesday of each month
    - Provides a technical overview of the security landscape of the organisation:
        i. Security Summary
        ii. Endpoint Protection
        iii. Email Filter
        iv. Web Filter
        v. SOC/SIEM (SOCaaS)
        vi. Vulnerability Scanning

c. Daily Backup Report

- Status of backups, latest backup, and previous occurrences within the calendar month.

d. Self Service Ticket Review
    - Customer access to review the tickets open for their organisation within The Contractor's service desk.

6 Contract Management

The contract will be reviewed annually on or near the anniversary date. Revisions, amendments of the schedule will be reviewed and signed off by both parties. Performance of the contracted services will also be reviewed and signed off as part of this contract management process.

The financial and services schedules referenced in the contract are flexible and will evolve as per The Contractor and Customer Requirements during the contract period.

7 Billing

The Contractor will process and issue invoices for contracts on a Monthly billing profile on the 1st of the billing period unless informed otherwise or unless other billing arrangements are already in place.

Invoices for contracts on a Quarterly or Annually billing profile will be processed and issued a month in advance of the billing period.

The Contractor's invoices are due and payable in sterling 30 days from the date of the invoice. If an invoice becomes overdue for payment the full outstanding amount becomes overdue and payable. All contracts are accepted and fulfilled subject to terms and conditions of sale.

8 Licensing

The Contractor will provide Microsoft Licensing under the Microsoft Services Provider License Agreement (SPLA) program and under the Microsoft New Commerce Experience (NCE) program. Licenses procured via or through this program will be charged separately. Licenses under the SPLA program are non-perpetual (or subscription) licenses that can be used during the term of this

agreement. The Terms and Conditions of the SPLA program are beyond the control of The Contractor and The Customer will be bound by the terms provided via Microsoft. These terms are liable to change but are currently available for review via: https://www.microsoft.com/en-gb/Licensing/licensing-programs/spla-program.aspx Any other licensing that is procured or managed by The Contractor will be delivered in line with the manufacturer conditions and billed in line with the Monthly Subscriptions contract.

If applicable, please refer to the Financial Schedule for details of Microsoft Consumption.

9 Documentation

The Contractor will maintain completed and up to date documentation of The Customer's IT estate. This documentation is limited to the systems and services under support.

Documentation includes information for:

- Customer Contacts
- Infrastructure (Servers, Network etc.)
- Project Documentation
- Applications
- Processes and forms

The Contractor is responsible for ensuring that the documentation is reviewed and updated on a regular basis or as and when material changes occur.

10 Asset Management

The Assets Management process is for managing I&T assets through their life cycle to ensure that using them delivers value at optimal cost; they remain operational, fit the purpose, they are known and protected. Ensure that those that are critical support service capability are reliable and available.

It includes Software Licenses Management to ensure the optimal number of them are acquired, retained, and deployed within required business usage and installed software to meet license agreements compliance.

10.1.1 Service Provision

The Contractor will:

a. ensure documentation of supported assets
b. ensure management and optimisation of assets
c. ensure efficient use of software licenses
d. ensure asset classification
e. manage the asset lifecycle
f. provide reports for assets when required by The Customer