Metrea
Mission Data

C4ISR INTEGRATION
SERVICES DEFINITION DOCUMENT

April 2024

Version V1

Submitted by Metrea Mission Data Ltd
Head Office: Malvern Hills Science Park
Geraldine Road, Great Malvern, Worcestershire, WR14 3SZ, UK
Tel: 01684 878170 Fax: 01684 878171
E-mail: info@mmd.metrea.aero
Web: metrea.aero/mmd

Metrea

CORPORATE RELEASE STATEMENT

RELEASE

Action	Name	Role	Date
Prepared by	Sarah Williams	Bid Manager	April 2024
Reviewed by	Matt Spry	Solution Development Manager	April 2024
Authorised by	Simon Hancock	Technical Director	April 2024

DISTRIBUTION

Copy Number	Location	Name/Agency/Company
1	File	MMD
2	G-Cloud 14 Application	Crown Commercial Services

CHANGE HISTORY

Version	Date	Change Details
V1	April 2024	Final Version

COPYRIGHT

CONTENTS

1 Service Description

1.1 Service Overview

1.1.1 Metrea Mission Data's (MMD)G Cloud C4ISR Integration service enables Defence customers to create cloud-based solutions across complex Computers, Communications Command and Control, Intelligence, Surveillance and Reconnaissance (C4ISR) information exchange requirements. The service improves the collation and access to decision quality C2 data and the Processing, Exploitation and Dissemination of digital ISR inputs.

1.2 Service features

- Concepts and Requirements analysis & development. List X facilities
- Operator training in the use of cloud based ISR solutions
- Systems design using operational experts: Space, EW, C2, ISR, Cyber
- Independent technology and capability maturity assessments and audit
- Technical support with ISR imagery cataloguing and archiving solutions
- ISR services for reduced communications bandwidth and disadvantaged users
- Policy and Standards compliance, advice and design support
- ISR data visualisation services for Command and Control
- Information Assurance, Security and Cyber support, ISO 27001
- Safety Case Development and Review.

1.3 Service benefits

- Reduced capability integration risk of sensor data into exploitation systems
- Reduced acquisition costs through common technologies and shared solutions
- Increased analytical capacity across ISR systems
- Improved interoperability and STANAG compliance
- Increased options for dynamic process upgrades and reuse of data
- Faster consideration of technology choices
- Enhanced C4ISR system security and resilience
- Reduced training and implementation costs to buyer.

1.4 How the Service works

1.4.1 MMD Software Services help buyers plan how they will implement Integrated Electronic Surveillance (IES) cloud software services by providing suitably qualified and equipped business analysts, solution designers and security architects. Our uniquely experienced consultants have experience of working across this domain, managing the specific challenges to adoption of cloud services, particularly given unique security constraints. We ensure departmental policies for the adoption of Defence cloud services are considered as part of service planning, including compliance with appropriate Joint Service Publications. The user's requirements, concept for use and environment in which the services will need to exist are independently assessed against options for cloud technology. Formal plans are produced to document cloud options and to manage risks from cloud service adoption or migration.

1.5 What the Service works with

- Integrated Electronic Surveillance (IES) Cloud
- Maritime Situational Awareness Capability (MSAC) Clouds
- Electronic Warfare (EW) Clouds

- Maritime Domain Awareness (MDA) Clouds.

1.6 Service on-boarding support

1.6.1 MMD helps buyers plan how they will support ISR integration programmes with Defence cloud hosting and cloud software services by providing suitably qualified and equipped business analysts, solution designers and security architects. Our uniquely experienced C4ISR engineers and operators have consultancy experience across the unique Defence domains, which bring specific challenges to adoption of cloud services, particularly given unique security constraints. We ensure departmental policies for the adoption of Defence cloud services are considered as part of service planning, including compliance with appropriate Joint Service Publications. The user's requirements, concept for use and environment in which the services will need to exist are independently assessed against options for cloud technology. Formal plans are produced to document cloud options and to manage risks from cloud service adoption or migration.

1.7 Set-Up and Migration Support

1.7.1 MMD helps buyers to integrate to the cloud and between cloud services for Defence customers. Having supported planning, we configure cloud services, conducting testing, experimentation, exercising and trialling of the target cloud environments to ensure they are appropriately configured and operating in accordance with required Defence policy and accreditation statements prior to any migration. We evaluate cloud services for compliance with Defence organisation procurement requirements and scrutiny. We migrate user environments and data on behalf of the user community, ensuring transition plans including parallel operating is coherently managed. Our systems architects and technical staff conduct verification and validation activities to ensure data integrity has been maintained during migration and that network services are operating reliably. We provide monitoring of system performance to ensure KPIs are being adhered to.

1.8 Quality Assurance and Performance Testing

1.8.1 MMD helps buyers by providing independent assurance of the quality and performance of their cloud services. We conduct technology maturity assessments and then qualitative and quantitative analysis of performance, incorporating all aspects of capability integration. We use C4ISR specialists with Defence cloud expertise alongside technical engineering experts fully conversant with the appropriate Defence standards (MIL-STD, STANAG, etc.). Quality and assurance are reported on in terms of business effect at the capability level, covering such key areas as international Defence interoperability and adherence to community norms for near-real-time data integration and exchange.

2 Service Reporting and Management

- A monthly reporting cycle is used for the review of the measured performance against the Service Level Agreement (SLA) Key Performance Indicators (KPIs)
- The KPIs are reported to the Customer in the IES Programme’s Monthly Progress Report.

2.1 System Performance Indicators

2.1.1 In order to monitor the ongoing stability of the system and to allow future support planning, the System Performance Indicators (SPIs) detailed in Table 1 are monitored and reported on in the monthly reports.

SPI	Title	Description
1	SPRs Raised - Monitor Period	Total number of SPRs raised during the current monthly monitoring/reporting period.
2	SPRs Raised - SLA Period	Total number of SPRs raised since SLA was initiated.
3	SPRs Raised - Monitor Period and Item	Total number of SPRs raised against a specific item/system component during the current monthly monitoring/reporting period.
4	SPRs Raised - SLA Period and Item	Total number of SPRs raised against a specific item/system component since SLA was initiated.
5	SPRs Raised - Monitor Period and Priority	Total number of SPRs raised at each priority level during the current monthly monitoring/reporting period.
6	SPRs Raised - SLA Period and Priority	Total number of SPRs raised at each priority level since SLA was initiated.
7	Mean-Time-To-Recover - Monitor Period and Item	The average time to resolve a support issue for support issues raised against a specific item/system component during the monthly reporting period. The time is calculated from the time the support call/email was received to the time at which the support engineer has confirmed with the user that the issue has been resolved.
8	Mean-Time-To-Recover - Contract Period and Item	The average time to resolve a support issue for support issues raised against a specific item/system component during the SLA contract period. The time is calculated from the time the support call/email was received to the time at which the support engineer has confirmed with the user that the issue has been resolved.
9	Site Visits - Monitor Period	Number of on-site visits required to be made by the support engineer during the current monthly monitoring/reporting period.
10	Site Visits - SLA Period	Number of on-site visits required to be made by the support engineer since SLA was initiated.

Table 1: Monitored SPIs

2.2 Fault Categorisation

2.2.1 In order to monitor the failure types the fault categorisations detailed in Table 2 are used to identify the generic failure type for each issue.

Category	Description
No Fault Found	Support call was raised in error and no fault with the system or associated external systems was identified.

Category	Description
External System Impact	Support call was raised due to system failure caused (directly or indirectly) by and external system or data feed failing – e.g. loss of data feed.
Hardware Failure	Support call was raised due to a specific item of system hardware failing – e.g. disk failure.
Software Failure	Support call was raised due to a software fault – e.g. software bug where system does not perform as expected.
System Failure	Support call was raised due to an issue with the system configuration or system resources – e.g. hard disk full.
Admin Function	Support call relates to performing a system administrator function – e.g. password reset, user account creation etc.

Table 2: Fault Categorisations

2.2.2 The fault categorisation is made by the Integration Support Team on initial review of the support issue.

2.3 Key Performance Indicators

2.3.1 Table 3 provides the details of the KPIs that will be monitored and reported and used to assess the performance of the support in respect to the SLA.

KPI	Title	Description
1	Mean-Time-To-Recover - Monitor Period	The average time to resolve a support issue for support issues raised during the monthly reporting period. The time is calculated from the time the support call/email was received to the time at which the support engineer has confirmed with the user that the issue has been resolved.
2	Mean-Time-To-Recover - Contract Period	The average time to resolve a support issue for support issues raised during the SLA contract period. The time is calculated from the time the support call/email was received to the time at which the support engineer has confirmed with the user that the issue has been resolved.

Table 3: Monitored KPIs

3 Service Scope and Definition

3.1 Support Types

3.1.1 Table 4 provides an overview of the details of the different support level categories.

Title	Description
First Line Support	Support will cover all preventative and corrective maintenance associated with the hardware and software of the system and also include system administration functions.
Second Line Support	Support will cover only corrective maintenance of software related issues raised with the system and exclude all system administration and hardware related issues.

Title	Description
Test, Trial and Reference Rig Support	Support covers only corrective maintenance of software related issues raised with the system and exclude all system administration and hardware related issues. Issues raised against Test, Trial and Reference Rigs will be excluded from the KPI performance targets and response and resolution of issues will be based on a best endeavours approach.
Remote Deployment Support	Support covers pre-deployment checks and fault identification on items returned to MMD.

Table 4: Support Type Categorisation

3.2 Scope of Service Support

3.2.1 Table 5 provides details of the support services included in each support type.

Support Activity	1st Line	2nd Line	Test Rigs	Remote
24/7 Phone Call Access *- user access to the 24/7 phone call service*	✓	✓		✓
C4ISR Integration Email Support Access *- user access to the IES Support Email*	✓	✓	✓	✓
C4ISR Integration CWE Access	✓	✓	✓	✓
Preventative Maintenance Hardware *- on site engineer supporting regular preventative maintenance tasks for the hardware components*	✓			
Preventative Maintenance Software/System *- on site engineer supporting regular preventative maintenance tasks for the hardware components*	✓			
OS Patching *- on-site engineer supporting roll-out of operating system updates*	✓			
AVG Updates *- on-site engineer supporting* roll-out *of anti-virus system updates*	✓			
System Patching *- on-site engineer supporting installation of system updates*	✓	✓		
Corrective Maintenance Hardware *- on-site engineer supporting hardware fault diagnostics and repair/replacement of faulty item*	✓			
Corrective Maintenance Software *- remote engineering supporting software fault diagnosis (excluding fault rectification)*	✓	✓		
System Administration *- remote engineering support for system administration functions*	✓			

Support Activity	1st Line	2nd Line	Test Rigs	Remote
Back-up / Recovery *- On-site engineering support to manage data back-ups and data recovery if required*				
User Management *- remote engineering support for system user account management*	✓			
Pre-deployment serviceability checks *- remote engineering support for pre-deployment serviceability tests*				✓

Table 5: Scope of Service

4 Responsibilities

4.1 Supplier Responsibilities

4.1.1 The Supplier provides and maintains the C4ISR Integration services used by the Customer.

4.1.2 Additionally, the Supplier will:

a. Respond to support requests within the timescales listed in Section 6
a. Take steps to escalate and resolve issues in an appropriate, timely manner
b. Maintain good communication with the Customer at all times
c. Provide problem diagnosis and resolution fault flow diagrams/documents (to aid operator self-diagnosis).

4.2 Customer Responsibilities

4.2.1 The Customer will use the Supplier-provided C4ISR Integration Services as intended.

4.2.2 Additionally, the Customer will:

a. Notify the Supplier of issues or problems in a timely manner
b. Provide the Supplier with access to equipment, software and services for the purposes of fault investigations and rectifications
c. Maintain good communication with the Supplier at all times
d. Provide Supplier with the results of self-diagnosis and problem resolution having followed fault flow diagrams/documents (to assist Supplier with tracking common issues and aid improvement of problem diagnosis and resolution fault flow diagrams/documents).

5 Support Methods

5.1 Support Method Description

5.1.1 Table 6 provides details of the support methods used to deliver the C4ISR Integration support.

Support Method	Description
Phone Support	Provides access to a support engineer via dedicated direct telephone number - classification Official Sensitive.

Support Method	Description
Email Support	Provides access to a support engineer via an email address - classification up to Official.
Collaborative Working Environment	Provides access to a support engineer via a CWE portal - classification up to Official.

Table 6: Support Methods

6 Response Times

6.1 Service Support Period and Target Response Times

6.1.1 Table 7 defines the Service Support Period for each of the support methods. This Service Support Period identifies the times at which the service method will be manned/monitored.

6.1.2 In addition, the Target Response Times for each support methods are defined. The Target Response Time will be the time by which an initial acknowledgment of the support issue raised will be made by the support engineer.

6.1.3 The response times will not be applicable to those systems under the Test, Trial and Reference Rig Support.

Support Method	Service Support Period	Target Response Times
Phone Support	24/7 365 days per year	24 Hours
Support Email	Standard UK Office Hours 09:00 - 17:00 Monday - Friday Excluding Bank Holidays	24 Hours
Collaborative Working Environment	Standard UK Office Hours 09:00 - 17:00 Monday - Friday Excluding Bank Holidays	24 Hours

Table 7: Service Support Period and Target Response Times

7 Configuration Management

7.1 Disaster Recovery and Business Continuity

7.1.1 MMD mitigates against disaster through implementation of a dedicated Business Continuity Plan (BCP). The BCP covers the full range of Services provided by the Company and is exercised and challenged regularly at desk-top level.

7.1.2 For its corporate software, niche software and associated Services, MMD undertakes monthly backups of all corporate data, network and device configurations. Configurations are stored in secure locations at both Customer's and MMD locations. Server backups are subject to discovery and compatibility with the existing backup provisions.

7.1.3 As a matter of course during the term of the Service, configuration backups are updated each time a change is made to the configuration of a network and/or device. These updated configurations are stored in the same off-site secure locations as above and supplement, rather than overwrite, the previously saved configuration.

7.2 Configuration and Change Management

7.2.1 MMD undertakes configuration changes to the supported software and network(s) as requested by the Customer or as part of an approved resolution to an Incident. Configuration activity can vary, although the following activities are examples of some of the actions that may be performed:

- Access-list and address translation modifications
- Routing protocol changes; and
- VLAN configuration changes.

7.2.2 Unplanned configuration changes will be made, subject to Change Management approval (retrospectively if the Incident is of sufficient severity), in line with the agreed incident resolution timeframe for the assigned incident priority.

7.2.3 Planned configuration changes will be made, subject to Change Management approval, in line with the agreed incident resolution timeframe for the assigned incident priority.

7.3 Patch Management

7.3.1 MMD undertakes the implementation of regular patches to the current Server and Network Device Operating System (OS) version on a regular basis (e.g. for security purposes) or as-required basis where a patch or upgrade is required to restore a service (as a result of an Incident) or to address a critical security breach.

7.4 Hardware Maintenance (Break/Fix) Support

7.4.1 MMD registers and manages hardware failure Incidents with the Customer and any 3rd Party hardware maintenance Supplier or vendor warranty in line with the 3rd Party Support Request Management process.

7.4.2 Where the recovery of a device follows the replacement of a failed hardware component which requires further support (for example the rebuilding and restoration of a server) MMD provides remote support for such activity where possible. Where on-site support is required to achieve full recovery, this activity will be chargeable under the On Demand On-Site Support service.

7.5 On-site Engineering Changes

7.5.1 MMD's Service is remotely delivered under normal circumstances. However, an on-site service engineering is available as a chargeable activity with the exception of monthly/routine pre-arranged site visits agreed in advance.

7.5.2 All requests for on-site Support Services are required to be logged via the Service Desk for appropriate registration and prioritisation. On-demand resources are available on a reasonable endeavour, next business day basis (Monday to Friday excluding English/Welsh public holidays) for requests received prior to 12 midday.

8 Information Assurance and Security Approach

8.1 MMD is a Cyber Essentials + (CE+) accredited Supplier. All MMD software and operational systems are designed, implemented and operated with the following approach:

- Secure by design and by default
- Least privilege as a default
- Follows NCSC guidance
- Standards-based ISMS (Information Security Management System) – certified to ISO27001 by ACM UK, a UKAS authorised certification body
- Current and maintained Cyber Essentials +; and
- Ongoing security assessment, internal audit and external audit of MMD ISMS.

8.2 The following high-level controls are implemented by default:

- Supplier security management
- Multi-factor authentication
- Conditional access
- IP address restricted access where appropriate
- Disk and data encryption for laptops and mobile devices
- Appropriate policies and procedures including change control; and ongoing staff training to aid the continual improvement of Information Security.

9 Pricing

9.1 Standard Charges – Rate Card

9.1.1 The following standard pricing options will apply for call-off activities:

Task / Resource Level	Hourly Rate	Day Rate
IT Consultancy – Director	£236.00	£1,774.00
IT Consultancy – Technical Consultant	£223.00	£1,674.00
Desktop Support – Remote	£74.00	£553.00
Desktop Deskside Support - Onsite	£74.00	£553.00
Server/ Network/ 3rd line Engineer	£110.00	£828.00
Application Specialist	£223.00	£1674.00
Cyber Security Consultant	£167.00	£1255.00
Solutions Architect	£223.00	£1674.00
Project Coordinator	£110.00	£828.00
Project Manager	£167.00	£1255.00

9.1.2 A Full Day is considered to be 09:00 to 17:00 (including 0.5-hour lunch). A Half Day equates to up to 4 hours of activity.

9.1.3 Project activity delivered outside of 09:00 to 17:00 Monday to Friday and Saturdays will be charged at 1.5 x standard rate. Project activity delivered on a Sunday and on Public Holidays will be charged at 2 x standard rate.

9.1.4 On-site work will be charged at the standard pricing rates with travel and accommodation subsistence costs payable.

10 Governance and Escalation

10.1 Governance Board

10.1.1 To ensure a positive and enduring relationship is maintained, the Supplier and the Customer convene a Governance Board on an annual basis to review the following items:

- Overall Service Performance
- The Customer's Operational Requirements and Business Strategy
- The Customer’s IT Strategy
- An assessment the appropriateness of the Service Agreement; and
- Identification of areas where MMD can provide further enhancement to the Customer’s business and/or IT strategy objectives.

10.2 Operational Service Review

10.2.1 Operational Service Reviews are held on a monthly basis via video conference or face-to-face to review the on-going performance of MMD’s Services. The Operational Service Review Board will meet in person, or via voice conference, and meetings will consist (at a minimum) of the Customer’s Operational Sponsor and Lead Scientific/Technical Advisor (or equivalent role/representative) and the nominated MMD Account Manager.

10.2.2 Items discussed at the Operational Service Review include:

- Service Performance Review (against SLA);
- Review of Infrastructure Health;
- Review of Trend Analysis Report;
- User Experience Assessment (Customer Satisfaction survey results);
- Contract Review (Contracted Devices);
- Dispute Resolution (and any areas of concern); and
- Continuous Improvement Programme Review.

10.2.3 The MMD Account Manager records the key issues discussed at the Service Review and any actions arising. The minutes are circulated to all parties within 10 working days of the meeting. The minutes are reviewed at the following meeting and updates provided accordingly.

10.3 Service Reporting

10.3.1 MMD provides the Customer with monthly Service Reports to demonstrate that services are being delivered successfully. Reports are published to the Customer within 10 working days of the end of the previous month. The report may be reviewed via voice conference at a time following publication suitable to MMD and the Customer (although it will most likely be reviewed during the Service Review meeting).

10.3.2 Items to be included in the monthly Service Report will include:

- Service Desk Contact Volumes
- Support Request Volumes
- Performance against SLA
- Telephone Help Desk Statistics; and
- Customer Satisfaction Survey Results.

10.3.3 Where service level breaches have occurred the MMD Account Manager provides requisite mitigation or justification information.

10.4 Continuous Improvement Programme

10.4.1 MMD provides a continuous improvement in two forms:

- MMD provided service improvement; and
- Customer-focused infrastructure improvement.

10.4.2 MMD continually strives to enhance the services provided to the Customer via a mix of tools, process and people development. As part of the Operational Service Review process MMD will demonstrate to the Customer the steps that are being taken to enhance services, and where appropriate demonstrate enhancements through improved service reporting metrics.

10.4.3 MMD also works with the Customer to advise and recommend improvements to the Customer's capability infrastructure. These recommendations include adding resiliency, improving reliability, addressing hardware and software obsolescence, and enhancing the user's overall experience. This process runs in line with the Operational Service Review process.

10.5 Contract Management

10.5.1 Variations to the schedules and charges are managed through Variation Charges outlined above. Variations will be recorded through the service desk and presented as part of the monthly reporting pack.

10.6 Escalation

10.6.1 The Customer should use the following path to escalate Business As Usual (BAU) support issues:

- Level 1 – MMD Service Desk Lead Engineer;
- Level 2 – MMD Service Desk Manager;
- Level 3 – MMD Head of Projects;
- Level 4 – MMD Technical Director;
- Level 5 – MMD Commercial Manager; and
- Level 6 – MMD Managing Director.

10.6.2 Issues arising which relate to the Service Agreement should bypass Level 1 escalation.

10.7 Key Personnel

10.7.1 The key personnel engaged within the delivery of this Service to the Customer are as follows:

Level	Name	Role
1	Alex Swift	Service Desk Lead Engineer
2	Dave Lawrence	Service Desk Manager
3	Alison Wright	Head of Projects

4	Si Hancock	Technical Director
5	Beth Roche	Commercial Manager
6	Owen Varley	Managing Director

11 Data Processing Agreement

11.1 Data Protection

11.1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

11.1.2 Schedule 7 of the GCloud Call Off Contract sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of personal data (as defined in the Data Protection Legislation, Personal Data) and categories of Data Subject.

11.1.3 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the data controller and the Supplier is the data processor (where Data Controller and Data Supplier have the meanings as defined in the Data Protection Legislation).

11.1.4 The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Supplier for the duration and purposes of this agreement.

11.1.5 The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

11.1.6 The Supplier shall, in relation to any Personal Data processed in connection with the performance in the supply of this Service:

- Process that Personal Data only on the written instructions of the Customer unless the Supplier is required by the laws of any member of the European Union to process Personal Data (Applicable Laws). Where the Supplier is relying on laws of a member of the European Union or European Union law as the basis for processing Personal Data, the Supplier shall promptly notify the Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Supplier from so notifying the Customer;
- Ensure that it has in place appropriate technical and organisational measures (available on request) to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data having considered the following:

  i. Nature of the Personal Data to be protected
  ii. Harm that might result from a data breach
  iii. State of technological development; and
  iv. Cost of implementing any additional measures.

- Ensure that all personnel and third party personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential, are aware of any comply with the Supplier's duties under this clause , are subject to appropriate confidentiality provisions with the Supplier or any Sub-processor, are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third part unless directed in writing to do so by the Customer or as otherwise permitted hereunder and have undergone adequate training in the use, care, protection and handling of Personal Data;
- Immediately notify the Supplier if it receives:

  i. A Data Subject Access Request relevant to the Customer or Supplier
  ii. A request to rectify, block or erase any Personal Data relevant to the Customer or Supplier
  iii. Any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation; and
  iv. Any communication from the Information Commission or any other regulatory authority in connection with Personal Data relevant to the Customer or Supplier.

- Not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Supplier has been obtained and the following conditions are fulfilled:

  i. the Supplier or the Supplier has provided appropriate safeguards in relation to the transfer
  ii. the data subject has enforceable rights and effective legal remedies
  iii. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
  iv. the Supplier complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

- Assist the Supplier, at the Supplier's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- Notify the Supplier without undue delay on becoming aware of a Personal Data breach;
- At the written direction of the Supplier, delete or return Personal Data and copies thereof to the Supplier on termination of the agreement unless required by Applicable Law to store the Personal Data; and
- Maintain complete accurate records and information to demonstrate its compliance with this clause 1.
- Cover all costs associated with any data breach arising from the Supplier or any sub-processors
- Operate their environments in line with and certified to at least the current versions of Cyber Essentials and ISO27001 standards and be externally governed where appropriate. The Supplier also retains the right to audit the Supplier and sub-processors on an annual basis.

11.1.7 The Supplier is responsible for:

- Ensuring Data Subjects have given appropriate consent to the processing of any Personal Data by the originating Customer; and

- Ensuring appropriate security measures are in place to meet current UK Data Protection Legislation.

11.1.8 It is accepted by the Supplier that before allowing any Sub-processor to process any Personal Data related hereto the Supplier must give the Supplier at least 30 days' notice in writing of the intended Sub-processor and processing.

11.1.9 For the avoidance of doubt, notwithstanding anything to the contrary in the Original Agreement, each party accepts liability for loss of Personal Data to the extent that the loss of Personal Data is caused by:

- A material breach by such party of their data processing obligations under Data Protection Legislation; and
- A failure by such party to provide the Security Measures that it was contractually committed to provide in relation to such Personal data.

Processing by the Supplier	**Details**
Scope of Processing	MMD processes personal data for the purposes of contract fulfilment with regards to agreed scope of services only, which is that of providing IT Services and normal business Operations
Nature	To be completed by Supplier
Purpose	MMD processes business contact information for the purposes of responding to support requests and contacting nominated employees regarding services incidents and alerts and for the purposes of carrying out the network support services contract as agreed with our Customers. Our Suppliers may subsequently process this data for us under our direction for the purposes of fulfilling our contractual obligations with our Customers. We may also process our Customers Customer data which can include a varying amount of personal data for Business to Consumer transactions, depending on the nature of the Customer.
Duration	The duration of processing is the length of the currently agreed contract.
Types of Personal Data	Names, Business email address, Business office locations, IP address information, internet use information including websites visited, times of internet access, times of computer use, Business telephone numbers, device names, National insurance numbers, dates of birth,
Categories of Data Subject	As required
Data return or destruction date(s)	As required