Service Definition Document

MS InfoTech Ltd

Version 2.7

Registered Office: 105 Regent House Business Center, 13-15 George Street, Aylesbury, HP20 2HU
Registered in England and Wales no: 8513709 VAT: 165 4436 02
Web: www.msit.co.uk E-mail: contact@msit.co.uk

Table of Contents

1. Purpose

This document provides details of our service arrangements. Included are the service packages, service levels, service deliverables, service transition, service connectivity, service changing policy, and additional services.

2. Service Overview

MSIT is responsible for designing, developing or maintaining associated services agreed upon during the service contract agreement.

MSIT can provide 24x7x365 monitoring and support services for various software and systems. MSIT monitors, supports and manages the agreed customer estate using ITIL® compliant processes;

All monitoring, support and management activities are performed remotely through secure internet or WAN connectivity, on-site support can be provided based on project requirements.

MSIT's proven monitoring support and management solution delivers:

- Dedicated ServiceDesk
- Automated monitoring of devices
- Self-service support and Self-service monitoring portals
- A named Service delivery manager to coordinate delivery and provide regular customer reports
- Fault co-ordination and resolution
- Incident management and resolution
- Problem management through trend analysis and environment management
- Change and configuration management to maintain the service in line with business needs.

3. Service Package

This chapter summarises the service scope, processes and capabilities.

Objective	To deliver monitoring, support and management of the customer's in-scope estate.

Scope	The service applies to an agreed list of in-scope items referred to as *CI* (that is, *Configuration Items*). MSIT document and maintain the definitive list of CIs in the *Service Operations Manual* during the *Service Transition* phase; this serves as the service's *configuration management database* for the contract term. **Note**: Each CI is located at a *customer-site'*, this should not be taken to imply they are geographically located on customer premises necessarily. Throughout this document, unless otherwise stated, the term *customer-site* refers to a geographically local collection of in-scope customer networks, devices or resources, whether they are physically located on customer premises, in a MSIT or third-party provider *datacenter*, or in a MSIT or third-party public or private cloud.
Context	MSIT Service Management is available for a range of technology operations, selected from the *Premium Support Plus and Service Management – Service Operations Catalogue*, which defines: • The type of CIs monitored and supported (for example, Storage, Backup or cloud operations) • The specific *feature sets* applicable to the CI type.
Feature sets	MSIT offer various feature sets for each area of technology operations (for example, for storage there is a mandatory *base feature set* for the controller, plus optional feature sets such as data protection, hosts and storage switches). Customers select which feature sets to include in their service package.
Supported-from	All support and management are delivered remotely from a secure, accredited MSIT operations center.
Required connection types	• Monitoring traffic uses secure TLS links over public internet between MSIT and the customer-site(s) • Support and management traffic use secure internet site-to-site IPsec VPN between MSIT and the customer-site(s).

Engagement	Customer engagement with the service is through the: • MSIT SDM for reporting, teleconference meetings and escalation • MSIT Service Desk; by email or telephone • MSIT Self-service support portal to create and-or update incidents and *change requests* • MSIT Self-service monitoring portal to view metrics and trends.
Service Desk	• Provides 24x7x365 support • Handles events, requests, queries and incidents relating to CIs, as raised by authorized users by phone, email or self-service support portal • Handles *change requests* in accordance with MSIT's Change Management process.

Self- service support portal	MSIT provides customer-nominated representatives with access to the Self-service support portal in order that they can: • Log and-or monitor issues • Raise and-or monitor *CRs* • View the *CMDB*.
Self- service monitoring portal	MSIT provide access to monitoring and statistical information.
Service capabilities	
Event management	Providing *near-real-time* device monitoring, alert handling and alert notification.
Incident management	Providing hardware *break-fix* and critical alert fault coordination, incident support, vendor liaison and Incident resolution.
Change management	Performing all tasks involving change in accordance with the MSIT Change Management process, which interacts with customer change processes as required.
Problem management	Providing regular incident trend analysis, which enables the identification of recurring problems and their root causes.
Capacity management	Monitoring and responding to *threshold breaches*, growth forecasts, maintaining adequate capacity for growth.

Maintenance	Applying patches, bug-fixes and upgrades to CI related software and-or firmware in line with best practice.
IT Service Continuity Management	Participation in *DR* documentation, contingency testing and in any actual recovery activity, in line with contractual scope.
Service Management and Reporting	Providing a named Service Delivery Manager, regular service review reports (and meetings) containing incident and change statistics and technical performance reports and health-checks.
Continual Service Improvement	Managing *service improvement plan*s which track recommendations for changes to improve service provision.
Configuration & Knowledge Management	• Maintaining the definitive agreed record of all CIs supported by this service in the CMDB, which is viewable through the MSIT Self-service support portal and also represented in the *SOM* • Maintaining a knowledge database to allow MSIT support teams to efficiently resolve known issues and find supporting information.

4. Service Levels

This section identifies the service level measures applicable to this service. The customer should consider these measures in the context of the general terms and conditions described in the contract document.

Response Time	• Incidents
	  ○ P1
	  ○ P2
	  ○ P3
	• Changes
	  ○ Standard
	  ○ Normal
	  ○ Emergency

5. Service Deliverables

This chapter describes what this service delivers to the customer. It should be read in conjunction with the appropriate technology-specific definition in the Premium Support Plus and Service Management – Service Operations Catalogue, which will define any technology-specific deliverables

5.1 Resources

Deliverable	Frequency	Description and content summary
ServiceDesk –contact number	Continuous	• MSIT provide the customer with a 24x7x365 service desk telephone number for the purpose of reporting incidents and raising CRs for Cis • Calls are logged on receipt, and will be acted upon within the customer's contractual service window • The Service Desk and Self-service support portal are accessible to named individuals only; not to the customer's users in general.
Self-service support portal	Continuous	The customer is provided with access to the Self-service support portal via the internet. Using the portal, the customer can: • Create new and update existing incidents for investigation • Create new and update existing CRs from a change catalogue • View their CIs on the CMDB MSIT provide each named individual with an account for their sole use, with their username being their email address. No shared accounts are provided.
Self-service monitoring portal	Continuous	MSIT provide the customer with access to the Self-service monitoring portal, showing monitoring metrics for in-scope systems, to allow customer administrators to view trends and manage infrastructure resources.

Configuration management database (CMDB)	Continuous	MSIT create and maintain a CMDB for all assets in scope of the contract and provide the customer with visibility of the contents through the Self-service support portal and the SOM
Named Service Delivery Manager (SDM)	Continuous	A named SDM is assigned to the customer, to provide: • Technical Service Review reports • Service Improvement Planning • Major Incident Reports

5.2 ITIL Processes

MSIT operates managed services in accordance with the ITIL framework for IT Service Management. The following sections contain the key deliverables relevant to this service.

5.2.1 Event Management

Deliverable	Frequency	Description and content summary
Near-real-time device monitoring	Continuous	• The MSIT Monitoring Platform ○ Performs continuous monitoring of customer systems, collecting metrics for analysis and reporting, and identifying alert conditions when thresholds are breached ○ Sends triggered alarms to the MSIT Service Desk, enabling appropriate remedial action to be taken • MSIT perform modification of alert sand thresholds as necessary

Alert Notifications	On alert	• Monitoring alerts are sent to the MSIT ServiceDesk for further investigation and can also be emailed directly to the customer if required • When a notification is received from the customer's monitored environment, MSIT alert customer chosen contacts, as agreed during
		the service transition stage and recorded in the SOM • Different contacts and methods of contact can be selected for different technologies, services, incident priorities, and times of the day/week/year, to make sure critical incidents are routed to the correct people, and that customer teams are not disturbed unnecessarily.
Monitoring configuration	Continuous	• MSIT monitor all systems in scope of the service using its standard probe configuration for each technology type by default • The customer may request that the metrics monitored and alarm thresholds used are changed to suit their requirements, except where the CIs are subject to an Availability Service Level
Event Handling	On alert	All alerts are processed by MSIT (not just critical alerts) and the appropriate action is taken to notify the customer and resolve the issue (if required)

5.2.2 Incident Management

Deliverable	**Frequency**	**Description and content summary**

Technical Service Desk	Continuous	The Service Desk: • Assists with software issues, firmware issues and hardware faults • Provides an escalation path for customer administrators when assistance is required.
Incident Reporting	Per Incident	• Customers may report incidents to the Service Desk by telephone, the Self-service support portal, or email • All Priority 1 (critical, service-affecting) Incidents must be reported to the Service Desk by telephone (rather than by using the Self-service portal or email), to ensure that they are acted upon immediately

		• Priority 1 incidents not reported by telephone are excluded from any contractual SLA • Incidents and changes logged by email are not bound by • *response time SLAs*, due to the indeterminacy of mail transit.

Incident Notification and Escalation	Per Incident	• MSIT notify the customer via email when an incident is created, updated or changed • The customer can specify preferred contacts to be informed by telephone, based on the priority and timing of incidents • MSIT document the nominated customer contacts for incident notification and escalation in the SOM.

Incident Response	Per Incident	• MSIT escalate alerts to its technical teams for investigation, while also informing the customer by the agreed preferred contacts • The customer must be available to provide assistance with any systems or applications not under MSIT's management that interoperate with the managed systems.
Pre-defined responses	Per Incident	MSIT and the customer agree predefined responses to be taken for common types of incident, for example restarting a service or expanding a storage container.
Emergency activity	Per Incident	For incidents categorized as P1, MSIT take the appropriate action required to restore operation or to prevent a system outage.
Response and actions	Per Incident	The customer shall provide timely feedback, always within seven days, to requests for information or action from MSIT.
Vendor liaison	Per Incident	If there is a need to involve product vendors, for log analysis or additional support, MSIT communicate with them directly on the customer's behalf and provides the customer with the vendor's recommendations.

Premium Support (Break- fix)	Per Incident	• Fault coordination for pre-agreed high priority alerts applies if requested by the customer. MSIT deal with the alert directly and escalate to the break-fix provider on the customer's behalf. If appropriate, MSIT can take remedial action through a remote support session It is assumed all CIs have a • *Premium Support* contract. Any CI which is not covered by MSIT Premium Support must have a break-fix contract provided by a third-party The customer is responsible for any remedial work after a part • • or device replacement, or after any other resolution provided by a thirdparty support provider, except for any activities covered under Service Management, such as verifying the health of the operating system after a part replacement.

5.2.3 Change Management

Deliverable	**Frequency**	**Description and content summary**
Change Control	As needed	• MSIT perform changes to modify CIs only when authorized to do so by an approved CR • Both MSIT and the customer can raise changes against the items listed in the configuration documentation. • All CRs are performed under the MSIT Change Management process, which will interact with the customer's change processes as required, including submission of CRs to the customer's *CAB* • MSIT maintain an *emergency CAB* capability 24x7x365, to facilitate management of emergency CRs.

Change Classifications	Continuous	• MSIT define a set of *Standard* change definitions and a set of • *Normal* change definitions • All *Unclassified* changes and changes classified as *Normal* • must be approved by the MSIT CAB.
Customer Change Managers	Continuous	Customers are expected to nominate change managers to engage with MSIT on the approval and timing of *Normal* changes.
Change Orchestration	As needed	MSIT may elect to use an *orchestration appliance* to perform some changes where compatible and appropriate.
Enabling new features	Continuous	The enabling of new features is not covered by this service by default. New features may require an update to the infrastructure design or architecture, which can be performed by MSIT on a separately chargeable, consultancy
Self-Service Portal	As needed	MSIT and their customers raise CRs using the MSIT Self- service support portal, which can also be used to, manage and track CRs.

5.2.4 Problem Management

Deliverable	**Frequency**	**Description and content summary**
Problem Management	Continuous	MSIT provide proactive problem management processes to help avoid recurring issues. Problem records are maintained in MSIT's CMDB and are tracked on each customer's SIP.
Incident Trend Analysis	Via Service Review Reports	*Trend analysis* helps to identify recurring problems and their root cause. Output from this analysis feeds into the Service Improvement and Service Review processes.

Customer-managed devices	Continuous	If MSIT identify that the root cause of a recurring incident, problem, known error or security issue is due to the configuration or health of system(s) managed by the customer, the customer is obliged to resolve the issue Until the issue is resolved by the customer, no *contractual SLA* related to it (or its area of influence) applies

5.2.5 Capacity Management

Deliverable	**Frequency**	**Description and content summary**
Threshold breaches	Per Alert	Unless otherwise requested by the customer, MSIT will increase capacity (where applicable) on any CI that generates an alert based on agreed monitoring thresholds.
Growth forecasts	Service Review reports	MSIT will provide a forecast of future growth in each Service Review report, based on monitoring information collected over the reporting period only.
		• Effective capacity management is only performed where sufficient spare capacity is available
Maintaining adequate capacity for growth	Continuous	For example, storage systems should have and retain sufficient spare capacity throughout the contract term to allow for at least 30% growth in data • As spare capacity is used, the customer will need to purchase additional capacity, or perform regular housekeeping tasks, on a regular basis throughout the contract term to maintain the agreed spare capacity level.
		Prerequisite 2: Ensure any provided storage capacity allows for 30% growth Responsibility 4: Maintain 30% headroom for growth throughout the term

5.2.6 IT Service Continuity Management

Deliverable	Frequency	Description and content summary
DR Documentation	Ongoing	MSIT provide content for inclusion in the customer's DR documentation for the recovery processes relating to all CIs for which the *Data Protection feature set* has been selected (where
		applicable), to ensure that the tested contingency procedure can be repeated if a true disaster event occurs.
		As part of *System Contingency Testing* (available only with the Data Protection feature set), and in conjunction with the customer's wider DR procedures:
System Contingency Testing for in-scope devices	Up to twice per year, on Customer request.	• MSIT perform any device related commands and tasks necessary to make the device and-or its data available in a *replicated system* • Tests must be performed within MSIT's normal business hours. Any testing required outside of these hours is chargeable. • Third-party or external DR applications are excluded from system contingency testing unless they are specifically listed in the Data Protection service feature set documented in the appropriate technology chapter in the ***Premium Support Plus and Service management Service Catalogue***. • System contingency testing to public cloud or third-party providers is excluded

Managed Systems Scope	Ongoing	• The scope of MSIT's involvement is strictly limited to performing activity on CIs for which the Data Protection feature set has been selected (where applicable) as directed by the customer in order to test or invoke DR • Other activity required for the customer's business to invoke contingency are excluded, and this service's element should be considered to be one part of the customer's business continuity plan.

5.2.7 Configuration and Knowledge Management

Deliverable	Frequency	Description and content summary
Configuration Management Database	Continuous	MSIT maintains a CMDB as the definitive agreed record of all CIs, which is also represented in the SOM.
IT Service Management System	Continuous	MSIT uses its *ITMS* to record all incidents and (or changes) occurring on CIs. Generated statistics are used in: • Reports identifying service level trends • Recommendations for service improvement • Incident trend analysis and service reviews.
Design documentation	Continuous	Where appropriate, MSIT maintain technical design and configuration documentation for the managed systems in scope.
Changes and updates	As required	MSIT maintain configuration documentation inline with the completed changes being performed. This includes modification to the existing configuration defined by the service feature set(s) selected.
Knowledgebase	Continuous	MSIT maintain an internal knowledgebase relating to each Customer's systems, and for each technology and system within the Premium Support Plus and Service Management – Service Operations Catalogue, to promote first-time fix and reduced incident resolution times.

5.2.8 Service Reporting

Deliverable	Frequency	Description and content summary
Service Review Reporting	Quarterly	• A formal, statistics-based Service Review Report is created by the Service Delivery Team and provided to the customer on a quarterly basis, appropriate to the level of service package selected • The report is sent by email to the customer by the named SDM, who will organize a Service Review meeting with the customer to discuss the report content.
Incident and Change Statistics	Quarterly	All Service Review reports include analysis of logged incidents and changes for in-scope systems over the reporting period, including: • Top categories of incidents and changes • Incident priorities • Methods by which incidents and changes have been logged • Incident resolution closure codes (for example, capacity increased or configuration modified) • A full list of all tickets raised, with MSIT's response times.
Response Time/SLA Monitoring and Reporting	Quarterly	• As part of the Service Reviews, a report is generated showing how MSIT's support teams have performed against the measured level. • System-generated reports can also be accessed through the Self-service support portal on an ad-hoc basis showing support response times and SLA adherence.

Technical risk reporting and recommendations	Quarterly	Service Review reports also include: • Capacity reporting and growth forecasting • System performance profiling • Risks identified by MSIT or by technology vendors • Technical observations and recommendations, including system upgrades

5.2.9 Continual Service Improvement

Deliverable	Frequency	Description and content summary
Service Improvement Planning	Continuous	• The assigned MSIT SDM maintains a Service Improvement Plan and works with the customer and MSIT technical teams to progress items raised on the plan • This plan typically contains the following: ○ Problem records arising from multiple repeat incidents of the same category or relating to the same CI ○ Remedial actions identified from major incidents
		○ Plans for upgrades or configuration changes ○ Future MSIT or customer requirements

5.3 Operational Activities

Deliverable	Frequency	Description and content summary

Planned maintenance	As required	• MSIT endeavor to provide, by email, advanced notification of any planned maintenance activities, either by MSIT or by its third-party providers, at least five working days in advance of the maintenance commencement • Where maintenance is required more urgently, to prevent a longer outage or a security incident, or due to third-party provider timescales, MSIT may give less notice than five working days • The customer must inform MSIT whenever they intend to perform any maintenance to sites, networks or other devices that may affect the availability, communicability, performance or integrity of any system monitored or managed by MSIT

		• MSIT apply firmware, upgrades and patches for OSs and supported host software (if the appropriate feature set is selected), to minimize the risk of: ○ Incidents occurring due to bugs ○ Security breaches due to known vulnerabilities

Patching and upgrades	As MSIT recommend or by Customer request	• All patching and upgrades are performed remotely. If the customer requires any on-premises activity, it is chargeable under a MSIT Professional Services contract • MSIT recommend upgrades or patches to the customer either: ○ In response to incident or problem tickets ○ Following scheduled health-check activities, as reported in Service Review reports ○ Where required to facilitate changes to other devices to retain interoperability ○ The customer may request patches or upgrades be applied where they are required for interoperability with other systems under the customer's management.
Health checks	Quarterly	• MSIT perform quarterly health checks on all managed systems to review performance, ensure sound configuration, review capacity, and identify any risks and recommended upgrades. • The findings of these health-checks form the technical sections of Service Review reports.
Change Management	Continuous	All patches and upgrades are planned and implemented according to the MSIT Change Management process.

5.4 Service Guides, Documents and Reports

The following service guides, operational documents and reports are provided to the customer by MSIT, and maintained as required throughout the lifecycle of the service:

Deliverable	Frequency	Description and content summary
Service Specification	Contract	A schedule of the customer's contracted services and associated charges.
Service Level Agreements	Contract	MSIT's standard Service Level Agreements.
Terms and conditions	Contract	MSIT's terms and conditions for all services.
Managed Service Transition Guide	Start-up	How customer services are transitioned into live operation.
Customer Prerequisites Guide	Start-up	The activities the customer must perform before the service can be commissioned.
Customer Service Operations Guide	Ongoing	A guide to how MSIT operate customer service, how to communicate with MSIT and how to best use the service.

Service Operations Manual	Ongoing	MSIT produce and maintain a *SOM* document, which details the scope of the services provided including: • Services and service levels • Customer contacts • Locations and environments • CIs • Change management contacts and classifications • Incident management processes and contacts • *Monitoring Thresholds* and defined event response actions • Regular scheduled operational activities • Data protection schedules.
Detailed Design Document	Ongoing	A technical design document detailing the design and configuration of in-scope CIs.
Service Review Report	Quarterly	A quarterly Service Review Report, as described in Section 4.2.8. The contents of this report can vary depending upon the technology and associated feature-sets in-scope; see the Premium Support Plus and Service management – Service Operations Catalogue for specific details.
Service Improvement Plan	Ongoing	• MSIT maintain a *SIP* for the customer's services, which logs and tracks the status of any technical or service issues highlighted by the customer or by MSIT in relation to the service provided • By agreement, the SDM may operate a regular telephone conference call with the appropriate representatives from the customer to review the status of the SIP.
Major Incident Report	Per Major Incident	• In the event that a major incident occurs, for which MSIT are responsible, MSIT provide a *MIR* detailing the following: ○ Timeline of the incident ○ Root cause analysis ○ Workarounds employed

		○ Remedial actions ○ Lessons learned ○ SLA status • MSIT aim to complete the MIR and deliver it to the customer within ten working days of the resolution of the incident
Service Transfer Policy	Contract	MSIT's policy for handling data and asset returns at end-of- contract.
Service Transfer Plan	End of contract	A plan for handling data and asset returns for the customer, in accordance with the Service Transfer Policy.

5.5 Meetings

The following meetings are held between the customer and MSIT as part of this service:

Deliverable	Frequency	Description and content summary
Service Review Meeting	Quarterly	A Service Review teleconference meeting is held between the customer, their assigned SDM and Account Manager to discuss the performance and use of the service, and identify any future requirements for expansion, integration or additional services. This meeting takes place following delivery, by email, of each period's Service Review report and covers the following agenda items at a minimum: • Review of performance against SLAs • Review of any high-impact Incidents or Problems from the reporting period • Review of capacity (where relevant) • Recommendations by MSIT for any nonessential remedial work or upgrades that should be considered • Review new technologies / services as appropriate • Overview from the customer of any relevant forthcoming projects and plans that may require assistance from MSIT

		• Overview from the customer of key priorities for the next period • Review usage and consumption of license entitlements where relevant • Review of the SOM, and any other service-specific documentation that requires regular customer review. • A review of system capacity growth, performance, risks and other technical observations and recommendations.
Service Improvement Plan Meeting	Weekly, Fortnightly or Monthly, as preferred by the customer	• MSIT hold a teleconference meeting to review the SIP with the customer • The frequency of this meeting is jointly agreed between MSIT and the customer and may be varied throughout the term of the contract as required.
Other Meetings by Request	Upon Request	MSIT join teleconference meetings and, according to availability, any other meetings requested by the customer. Meetings may involve third parties of either MSIT or the customer, but there must always be a representative of both MSIT and the customer in attendance.

6. Service connectivity

This chapter identifies how the service connects to customer premises for the purposes of remote monitoring, support and management.

Connection types	• All monitoring traffic traverses the public Internet using encrypted TLS tunnels • Monitoring requires an external public static IP address on the customer's (or a third-party or public cloud provider's) firewall; dynamic IP addressing is not supported • For all support and service management traffic, MSIT operate an IPsec VPN over the Public Internet or other dedicated WAN link between a MSIT datacenter and each of the customers' sites, to facilitate remote management, diagnostics and log collection. The VPN is established between MSIT's shared-platform firewalls and the customer's dedicated firewall or other shared or tenant firewall in a third-party or Public Cloud environment • Unless the customer's firewall is also under MSIT Service Management, the customer must provide appropriate technical resource to assist MSIT with the configuration of VPNs • In the event of VPN or WAN failure, a customer assisted *Remote Support Session* utility (for example, LogMeIn Rescue) is used for service management (as for Premium Support Plus).

7. Service transition

MSIT use a standard methodology for transitioning customer services into live operation.

This methodology is described in full in the Managed Service Transition Guide.

Health Check	As part of the contract start-up process MSIT perform a health check of all CIs (including recording the running configuration as appropriate) to ensure they are configured in an appropriate manner. The health check covers configuration best practices, risks, capacity, vendor support status and physical component health. Where devices are not configured to MSIT's best practices, and-or MSIT deems the current configuration to represent a risk to the availability or ongoing operations of those devices, the customer must remediate the configuration, or engage MSIT Professional Services to perform the remediation, which will be a chargeable activity
Monitoring Alarms	Following implementation of the required monitoring configuration, any alarm conditions that exists on systems managed by the customer (such as storage volumes breaching a capacity threshold) must be remediated prior to the service entering live operation. Each alarm may be addressed in one of the following ways: • The customer may resolve the alarm by modifying the configuration of the monitoring target or by reducing its utilization below the agreed alert threshold • MSIT and the customer may agree in writing to modify alarm thresholds or to suppress or entirely remove certain monitoring alarm definitions. Any such modifications are recorded in the SOM. The customer must resolve all outstanding alarms via one of the above methods within seven days of notification from MSIT; should the customer fail to do so, MSIT will commence recurring billing of the service but will not transition the service into live operation until the alarms are fully resolved.
Design and Documentation	• MSIT use existing customer design documentation (where available) for the CIs, and combine it with the running configurations recorded in the health check. This documentation is used by the MSIT Service Desk and by the customer as a basis of the Service scope. It is the customer's responsibility to ensure that any documentation provided to MSIT is accurate and current

	• MSIT provide neither system design nor configuration recommendations for customer systems outside the contractual scope of MSIT management

Meetings	**Service transition workshop** The customer is required to attend a Service Transition workshop and any further workshops required to complete the detailed service and technical design. The customer should provide the following representatives at this meeting: • Service owners and-or technical owners for any applications or systems that utilize the infrastructure to be managed by MSIT • Technical owners for any supporting infrastructure needed to allow MSIT to access and monitor the in scope CIs (for example, network engineers, for creating VPNs and firewall rules) • Project manager, if the customer has chosen to use one. **Project closedown** The customer is required to attend a project closedown meeting to formally close projects for transitioning new services into operation.
Data migration	Migration of workloads and datasets from legacy systems to systems under MSIT service management is not included in this service
Training sessions	• Using the Self-service support portal MSIT provide, on request, a single remote web-based training session to the customer's administrator(s) covering the access and use of the MSIT Self- service support portal, to supplement the instructions provided in the *Customer Service Operations Guide* • Using the MSIT Self-service monitoring portal MSIT provide, on request, a single remote web-based training session to the customer's administrator(s) covering the access and use of the MSIT Self- service monitoring portal, to supplement the instructions provided in the *Customer Service Operations Guide*

8. Service charging policy

MSIT Service Management is charged according to the types, sizes, and configuration of the CIs selected by the customer and the feature sets selected for those CIs. These selections are listed in the ***Customer Service Specification*** document; a minimum-commit charge is calculated based on the selections made.

During service transition, and throughout the life of the contract, the customer may choose to add additional CIs to the scope of this service; these are charged using the same metrics under a flexible-commit charge. Customers may flex up to 130% of the original number of CIs; MSIT reserve the right to require a ***Contract Change Note*** to adjust the minimum commit for any expansion beyond 130%.

9. Additional services

Customers should contact their MSIT Account Manager to discuss the available options, some of which are shown below .

Service Change	Adding new feature sets requires updating the service design and-or architecture. MSIT can perform this on a separately chargeable consultancy basis
Service upgrade	Service review upgrade – A quarterly remote service review meeting is included as standard. It can be upgraded to monthly and-or delivered onsite instead of via teleconference at additional cost.
Bespoke services	MSIT Professional Services can be engaged to assist with a range of bespoke services including, but not limited to: • Migration of workloads, datasets and monitoring configurations from legacy systems to systems under MSIT service management • Out of scope support – MSIT can provide support and professional services for out of scope equipment • Service transfer and end-of-life – Any bespoke activities required by the customer outside of the *Service Transfer Plan* can be provided using MSIT Professional Services – See also: *Service Transfer Policy*
	Technologies to which this service can apply include:

Applicable technology areas	• Backup operations • Hypervisor operations • Networks operations • Public cloud operations • Storage operations • Server operations

10. Glossary

This glossary defines MSIT and service-specific terminology only. Industry standard acronyms are expanded on first use within the document and are not repeated here.

Term	Also known as	Definition
MSIT	MS InfoTech Ltd	
Availability SLA		Availability service level agreements, typically defined in terms of service uptime, are particularly applicable for infrastructure and service provision arrangement where a continuous IT service is provided.
Backup methods		The main backup types are: Full; Incremental; and Differential; but also include Continuous data protection and mirroring. In the context of this document Backup methods refers to the means of backup (that is the hardware or software infrastructure used).
Break-fix		Break-fix is a reactionary IT business support model in which the repair of an IT device or system component is done only when it fails (for example, a disk drive or server or router ceases to function).
CAB	Change advisory board	Delivers support to a change management team by approving requested changes and assisting in the assessment and prioritization of changes.

CCN	Contract change note	See – Contract change note
Change request	CR	A document requesting a change to an item within the scope of the contracted service, or to the service itself
CI	Configuration item	See – Configuration item

Clustering		Connecting two or more computers together in such a way that they behave like a single computer. Clustering is used for parallel processing, load balancing and fault tolerance.
CMDB	Configuration management database	See – Configuration management database
Collapsed core		Collapsed core networks are those where the distribution and core layer functions are implemented by a single device (a switch). In the context of this document it would require selection of the Core + Distribution feature sets for a device.
Configuration item	CI	A hardware, firmware, software or other item monitored, supported and-or managed by MSIT. That is, it is included in the agreed list of in-scope items as an item covered by the selected service
Configuration management database	CMDB	A repository for information technology installations. It holds data relating to a collection of IT assets
Contract change note	CCN	Contract change notes are used to document amendments to contractual commitments during the contract term

Contractual SLA		A Contractual service level agreement defines the boundaries of responsibility between customer and supplier, sets standards of performance and defines the measurement of service performance. It commits the supplier to delivering to required service levels and identifies the consequences of failure, usually in the form of service credits or other compensation.
CR	Change request	See – Change request
	Customer service	See – Customer service operations guide

CSOG	operations guide	
Customer service operations guide	CSOG	The Customer Service Operations Guide. A guide to how MSIT operate customer service, how to communicate with MSIT and how to best use the service.
Customer service specification		Defines the service configuration to be deployed for a specific customer
Customer support server		The Customer Support Server is a MSIT provided remote server used for remote service management activities
Customer-site	Site	Customer-site refers to a geographically local collection of in- scope customer networks, devices or resources, whether they are physically located on customer premises, in a MSIT or third-party provider datacenter, or in a MSIT or third-party public or private cloud.
Datacenter	DC	A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems

DD Boost	EMC Data Domain Boost Open Storage	See – EMC Data Domain Boost
Disaster recovery	DR	The process of restoring and assuring the continuation of essential IT services in the event of a disaster disrupting normal operation/
DR	Disaster recovery	See – Disaster recovery
EMC Data Domain Boost	DD Boost Open Storage	EMC Data Domain Boost software is designed to offload part of the Data Domain deduplication process to a backup server or application client. It is based on Symantec's OST (Open Storage) technology protocol.
		Exclusions are, for the purposes of this document, items outside of the scope of this

Exclusion		service contract for which MSIT are not liable.
Feature-set		A feature or collection of features attributed to a device (for example a storage controller) that describe that device's function (for example, Controller) and elements of the device (for example, Data Protection) to be monitored by MSIT.
Feature-set; Base		A feature-set that defines the item's base functionality (for example, controller or operating-system).
Feature-set; Data protection		A feature-set that defines the item's data protection features.
Fully collapsed		Fully collapsed networks are those where the access, distribution and core layer functions are implemented by a single device (a switch). In the context of this document it would require selection of the Core + Distribution + Access feature sets for a device.

Hierarchical internet working model		Hierarchical networks are those where the core, distribution and access layer functions are implemented by separate devices (switch) with dedicated functionality. In the context of this document it would require selection of the Core, Distribution or Access feature set as appropriate for each device type.
Term	Also known as	Definition
IPMI	Intelligent platform management interface	IPMI is a set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI) and OS
ITIL	Information Technology Infrastructure	A set of practices for IT service

	Library	management that focuses on aligning IT services with the needs of business.
ITMS	IT Service Management system	The system used by the MSIT Service desk to manage events, incidents, problems and changes
Major incident		The parties and process for declaring an incident a major incident is agreed during service transition. Whilst no formal ITIL definition exists these are typically incidents with significant corporate impact over and above a P1 incident, which do not require invocation of disaster recovery.
Major incident report	MIR	Major incident reports identify incident timeline, root cause, workarounds and-or remedial actions and lessons learned
MIR	Major incident report	See – Major Incident, Major incident report

Monitoring threshold		The monitoring threshold is the trigger value beyond which an alert will be raised. See also – threshold breach
NAS	Network attached storage	Typically a NAS is a single storage device that operates on data files
National operations center	NOC	A location from which MSIT deliver their monitoring, support and or management services.
Near realtime		Near real-time (in telecommunications and computing) refers to the time delay introduced by automated data processing or network transmission between the occurrence of an event and the use of the processed data (for example, for display or feedback & control purposes).
NOC	National operations center	See – National operations center
		The program which, after initially loading,

Operating System	OS	manages the other programs in a (virtual) machine. The installed applications make use of the operating system. For example, Microsoft ® Windows ®, Windows Server ® and Linux ®
Orchestration appliance		A MSIT tool for automating standard changes and provisioning
OS	Operating System	See – Operating System
Prerequisite		Prerequisites are, for the purposes of this document, tangible resources, actions or commitments without which the service cannot be initiated and whose provision and maintenance (where applicable) is the responsibility of the customer for the duration of the contract.

MSIT Premium Support	PS	MSIT Premium Support is MSIT's proven break-fix support solution
MSIT Premium Support Plus	MSIT Premium Support Plus	MSIT Premium Support Plus is MSIT's proven monitoring solution
SLA	Service level agreement	An official commitment to the level of service provision that prevails between a service provider and their customer
SLA, Availability		See – Availability SLA
SLA, Contractual		See – Contractual SLA
SLA, Response-t time		See Response time SLA
Software infrastructure server		Software infrastructure servers are, in this context, (physical or virtual) servers forming part of the service infrastructure and running application software (for example, backup software such as Simpana) required to deliver and manage the MSIT service.
SOM	Service operations manual	See – Service operations manual
Symmetric bandwidth		Bandwidth with equal upload and download speed
Threshold breach		In the context of the MSIT Monitoring Platform a threshold breach occurs when an event on a monitored item exceeds a preset threshold. For services that include monitoring, MSIT define these thresholds and agree them with the customer during the service transition stage, they are maintained throughout the contract term. See also – Monitoring thresholds

Trend analysis		Analysis of data to identify patterns. Trend analysis is used in problem management to identify common points of failure or fragile configuration items.