SERVICE SCHEDULE

ENTERPRISE INFRASTRUCTURE MANAGED SERVICE

Last Update: 29 September 2025

1. **General.** This is a Service Schedule setting out specific terms of Service in respect of BMIT's Enterprise Infrastructure Managed Service. The Enterprise Infrastructure Managed Service shall be considered to constitute a Professional Service, pursuant to Annex A5.

2. **Service Description.** The Enterprise Infrastructure Managed Service, provided by BMIT, covers both proactive and reactive support as outlined in this Service Schedule. It includes onsite, offsite, and remote activities related to deployment, administration, management, monitoring, support, and technical advisory services. The service is designed to establish, maintain, and ensure the proper and continuous functioning of the Customer's IT infrastructure, including systems administration, databases, networks, endpoints, and user environments.

3. **Proactive Support Services.** BMIT agrees to provide to the Customer the proactive services listed in this clause, subject to the prerequisites or conditions specified below. Such services are provided as Metered Professional Services as defined in Annex A5.

    a. Infrastructure services:

Proactive Support Services	Prerequisite/s or other conditions
Set-up central monitoring for the hardware, storage and network infrastructure utilisation and system logs	The Customer's infrastructure must support standard monitoring protocols, including but not limited to SNMP (Simple Network Management Protocol), and be compatible with advanced network technologies necessary for the deployment of monitoring solutions. Where applicable, the infrastructure must allow for the installation of monitoring agents. The Customer shall ensure that administrative permissions and technical conditions required for agent deployment are in place. Continuous and reliable network connectivity must be established and maintained between BMIT and the Customer's infrastructure to enable remote monitoring and data collection. The implementation of a logging service may incur additional costs to the Customer. These costs may relate to storage consumption, licensing, or third-party services. Furthermore, the volume of log ingestion will depend on the available storage capacity and the log retention policy configured by the Customer. The Customer is responsible for ensuring that sufficient storage resources are allocated to support the desired retention period.

Hardware updates	Due to the risk of a possible service disruption during such updates, BMIT recommends that such updates are performed during the Customer's low impact timeframe. Customer would need to advise BMIT the ideal timeframe in which such updates can be performed.
Provide utilisation and service reporting with recommended optimisations based on the usage and industry best-practices	The frequency of the report is agreed between both Parties during the initial scoping phase.
Technical infrastructure and architecture design review based on industry best practices, resources and/or requirements	The technical infrastructure and architecture reviewed will be such infrastructure and architecture as previously specifically agreed by BMIT.
Documentation of infrastructure including configuration	The frequency at which the infrastructure documentation (including configuration details, where applicable) is reviewed and updated shall be mutually agreed upon by both Parties during the initial scoping phase.
Network appliance audit and testing	The exact scope and frequency of the audit and/or testing is agreed between both Parties during the initial scoping phase.
External infrastructure vulnerability scan	The exact scope and frequency of such scan is agreed between both Parties during the initial scoping phase.
Perform infrastructure failover test	The exact scope and frequency of failover testing is agreed between both Parties during the initial scoping phase. The Customer must have a disaster recovery plan and an adequate solution to perform the failover.

b. System Administration services:

Proactive Support Services	Prerequisite/s or other conditions
Real-time monitoring of critical OS/ database management system (DBMS) services (or daemons) and system disk usage levels	The specific operating system and database services (or daemons) to be monitored will be such operating system and database services (or daemons) as previously specifically agreed by BMIT.
Monitoring and alerting of backup events	BMIT shall monitor the backup storage repository and the backup jobs. BMIT will attempt to resolve backup job failures arising from policy or application issues. However, BMIT shall alert the Customer of any critical alerts, or any intervention required.

Application of OS/ backup/ database (DB) upgrades, patches and service packs	The Customer shall agree with BMIT on a frequency schedule to perform such task. Any identified critical OS/backup/DB vulnerabilities will be captured as a Service Requests.
Endpoint OS security hardening review and recommendations	Endpoint must be governed or managed by an endpoint management solution. The Customer is required to agree with BMIT on a frequency schedule to perform such task.
Provide utilisation and service reporting with recommended optimisations based on the OS / backup / IP telephony / database management system (DBMS) usage and industry best-practices	The frequency of the report is agreed between both Parties during the initial scoping phase.
Perform backup recovery tests	The frequency of recovery testing is agreed between both Parties during the initial scoping phase.
Design of a backup strategy and architecture based on industry best practices	The backup strategy and architecture shall be designed during the initial engagement phase. Thereafter, it shall be subject to review on an annual basis or upon the occurrence of any major changes to the Customer's infrastructure or operational environment. The timing and scope of such reviews shall be mutually agreed upon by both Parties.
IP telephony audit	The frequency of the audit is agreed between both Parties during the initial scoping phase.

4. **Reactive Support Services.** BMIT agrees to provide to the Customer the reactive support services listed in this clause, subject to the prerequisites or conditions specified below. These services are delivered as Metered Professional Services, as defined in Annex A5, and are available upon the Customer submitting a valid Service Request through BMIT's Service Desk, in accordance with the terms of Annex A5.

   a. Infrastructure services:

Response Service	Prerequisite/s or other conditions
Physical installation and/or relocation, repair or initial contact with repair service for technical triage of hardware and repair coordination with respective hardware vendors	Hardware is purchased or is being leased from BMIT and/or is covered with an adequate support agreement or warranty with the respective hardware vendor.
Set-up of a network device such as a firewall, Load balancer, router, switches and access points, based-on the agreed deliverables, schedule and architecture with Customer	The technology or vendor to be used must be agreed upon in advance with BMIT. BMIT reserves the right to decline any setup that has not been approved beforehand.

Set-up the network infrastructure in scope to a customer specific network monitoring system, a security information event management system and/or an audit logging system	This service does not include the provision of any tools or solutions and is dependent on the Customer having acquired the necessary tools beforehand. At its discretion, BMIT may recommend specific tools or solutions to support monitoring and logging requirements and, upon the Customer's agreement, BMIT will source and implement such tools separately. The Customer shall be responsible for any associated costs.
Set-up the selected disk groups and RAID policy on the storage solution	The technology and infrastructure components to be used must be agreed upon in advance with BMIT. BMIT reserves the right to decline any setup that has not been approved beforehand.
Set-up the required host storage connectivity and access lists	The technology and infrastructure components to be used must be agreed upon in advance with BMIT. BMIT reserves the right to decline any setup that has not been approved beforehand.
Failure diagnosis, resolution and recovery of hardware, storage and network infrastructure, including escalation to vendor in case of critical issues	The technology and infrastructure components to be used must be agreed upon in advance with BMIT. BMIT reserves the right to decline any diagnostic or recovery activity that has not been approved beforehand.

b. System Administration services:

Response Service	Prerequisite/s or other conditions
Set-up of Operating System (OS)	Any OS licensing is to be provided by Customer or acquired through BMIT. The OS version to be set-up must be agreed with BMIT and must be within the respective vendor's mainstream support and appropriately covered with extended support from the vendor, to allow escalation for critical issues.
Set-up an Anti-Virus (AV) or Endpoint Protection Platform (EPP) on the system	The Customer shall provide BMIT with an EPP solution or acquire the applicable licenses or service from BMIT
Set-up a backup solution for the endpoint and/or database (DB);	The Customer shall provide BMIT with a backup solution or acquire the applicable service from BMIT.
Set-up of database management system (DBMS) and application tools, database (DB) clustering and replication if required, including security and access control to database and grants on database objects	BMIT can only support the following: - Microsoft SQL Server - MySQL Any DBMS licensing is to be provided by Customer or acquired from BMIT. The DBMS version to be set-up must be within the respective vendor's mainstream support and appropriately covered with extended support from the vendor to allow escalation for critical issues.

Set-up of IP telephony system and ongoing management and troubleshooting	The Customer shall provide BMIT with an IP telephony solution or acquire such solution from BMIT
System administration management tasks may include: • Administration of root or privileged access; • Management of network services (such as DHCP and DNS); • Administration of directory services; • Management of user access and authorisation; • Policy management for users and devices (such as Group Policy Objects); • Administration of file and storage services; • Management of drive mapping; • Administration of web server platforms (such as Internet Information Services (IIS) or Apache); • Administration of virtualisation platforms, including the associated physical server infrastructure.	The technologies and platforms to be managed and management tasks to be performed by BMIT shall be determined and mutually agreed by both Parties prior to service commencement and may be revised over the period of engagement to reflect evolving technology and business needs subject to prior agreement over such revision between the Parties.
Failure diagnosis, resolution and recovery of OS, backup applications and authentication issues	BMIT shall provide regular updates to the Customer in relation to the issue. Updates will also be provided when ticket is logged with the vendor (if applicable), when significant change in progress has been registered and when the incident has been resolved.
Perform data or infrastructure recovery on a best effort-basis	Prior to initiating any recovery activity, the Customer shall provide BMIT with a detailed recovery plan specifying the data and/or infrastructure to be recovered, as well as the intended recovery site or location. BMIT reserves the right to review and approve the proposed recovery plan. Recovery services shall only be performed if the plan is deemed acceptable and feasible by BMIT. Any recovery request not agreed upon in advance may be declined at BMIT's sole discretion.

5. **Prerequisite/s or other conditions.** The following terms apply in relation to the provision of the proactive and reactive support services:

a. **Permissions for management tasks:** Customer shall provide BMIT with the necessary level of access permissions to execute any of the proactive and reactive support services it has contracted for.
b. **Security Event:** BMIT may, at its discretion, take immediate action to reduce the impact or severity of a Security Event on the Customer's IT infrastructure within the scope of the Service. Customer shall provide access to BMIT on its infrastructure, to allow BMIT to perform diagnostics and repairs as needed.
c. **Security vulnerabilities:** BMIT is not liable for any Security Events including, but not limited to, Security Events which may originate from vulnerabilities on Operating Systems, applications or appliances on which it is offering proactive or reactive support services.
d. **Right Not to Manage or Support Non-Agreed Elements:** BMIT will provide the Service only for infrastructure, software, and other elements expressly agreed between the Parties and defined in a Work Order. BMIT may exclude from management or support any infrastructure, software, or other items proposed or provided by the Customer that have not been mutually agreed as suitable for Service delivery. Any additional tasks or items requested by the Customer shall only be considered "in-scope" if mutually agreed in writing by both Parties. In such cases, the Parties shall seek to find a mutually acceptable alternative.
e. **Management of third-party software/appliances:** The Customer shall be responsible for maintaining any subscriptions, licences, and support agreements for any software or appliance not included as part of the Service and not defined in a relevant Work Order Form. All software licences purchased by the Customer or provided by BMIT must remain in conformity with the applicable vendor terms of use. In the event of any breach of such terms, BMIT reserves the right to refuse to manage the Service.
f. **Backup integrity and recovery:** BMIT is not responsible for the integrity of the data within a backup job and any failures to restore data from these backup jobs. Customer is responsible to schedule recovery tests to validate a backup job and provide and make all the necessary resources (both human and infrastructure) available during the entire duration of the recovery process, as may be requested by BMIT. BMIT shall perform and monitor such recovery tests, and Customer agrees that it is the Customer's responsibility to validate that the restored data is valid and in a usable state.

6. **Services in scope.** The list of proactive services and systems in scope of the Enterprise Infrastructure Managed Service is defined and maintained in the Customer's Enterprise Infrastructure Managed Service documentation. Such documentation is maintained by BMIT and its content, and any change to it, is subject to approval by both Parties.

7. **Service Levels.** The Service Levels defined in Annex 28 – General Service Level Agreement shall apply for the Enterprise Infrastructure Managed Service.