# SPECIFIC CONDITIONS K3 – MICROSOFT 365 MANAGEMENT SERVICES

These Specific Conditions govern the Microsoft 365 Management Services that may be provided by the Company under an Order Form, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms & Conditions for the Supply of Products and/or Services (the "**Conditions**") and Specific Conditions X3 – Standard Operational Services, which shall be deemed to be incorporated into the Contract for the performance of any Microsoft 365 Management Services performed under these Specific Conditions.

## 1 DEFINITIONS

1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions:

| | |
|---|---|
| "Anti-Virus Management" | means the Services provided in accordance with paragraph 4.4; |
| "Application Security Update Management" | means the Services provided in accordance with paragraph 4.6; |
| "End User Service Desk" | means the service desk responsible for acting as the primary point of contact for the Customer's End Users and may be delivered by the Company, the Customer, or a third party; |
| "Fair Use Policy" | means the policy for the reasonable and fair use of the Microsoft 365 Management Services as set out in paragraph 10; |
| "Managed Endpoint Devices" | means the domain joined desktop, laptop and/or thin client devices identified in the Order Form as the Managed Endpoint Devices for the purposes of the Microsoft 365 Management Services; |
| "Microsoft" | means Microsoft Corporation and its affiliates; |
| "Microsoft 365 Compliance Centre Dashboard" | means that part of the Microsoft 365 Platform which shows compliance information for the Managed Endpoint Devices; |
| "Microsoft 365 Core Platform" | means the Microsoft 365 Platform tenancy, authentication and supporting features accessed by the administration centre portal; |
| "Microsoft 365 Management Services" | means the Services provided under these Specific Conditions; |
| "Microsoft 365 Platform" | means the Microsoft 365 platform as provided by Microsoft; |
| "Microsoft Defender ATP Dashboard" | means that part of the Microsoft 365 Platform which shows security vulnerability and threat information gathered by the Microsoft 365 Platform for the Managed Endpoint Devices; |
| "Microsoft EMS" | means Microsoft's "Enterprise Mobility and Security" intelligent mobility management and security platform; |
| "Microsoft EMS Dashboard" | means that part of the Microsoft 365 Platform which shows security statistics gathered by the Microsoft 365 Platform for the Managed Endpoint Devices; |
| "Microsoft Exchange Online" | means Microsoft's hosted email platform; |
| "Microsoft Feature Update" | means an Update to the Microsoft Windows 10 operating system which includes new features and which are typically released on a twice-yearly basis; |
| "Microsoft Feature Update Plan" | means a schedule agreed by the Customer and the Company in relation to the application of the Microsoft Feature Update to Managed Endpoint Devices; |
| "Microsoft Intune" | means Microsoft's cloud based mobile device management platform; |
| "Microsoft Out Of Band Security Update" | means an Update to address a specific critical security vulnerability in the Microsoft Windows 10 operating system or Microsoft Office client applications; |
| "Microsoft Quality Update" | means an Update to the Microsoft Windows 10 operating system or Microsoft Office Client Applications which are typically released on a monthly basis and includes security patches and bug fixes; |
| "Microsoft Quality Update Schedule" | means a process and timescale for the rollout of a Microsoft Quality Update to the Update Testing Group and Managed Endpoint Devices, agreed by the Customer and the Company in accordance with paragraph 4.5.1.2; |
| "Microsoft Reseller Relationship" | means the process of associating the Company to the Customer's Microsoft 365 account as defined by Microsoft; |
| "Microsoft Sharepoint" | means Microsoft's web-based collaborative platform; |
| "Microsoft Security & Feature Update Management" | means the Services provided in accordance with paragraph 4.5; |
| "Microsoft Teams" | means Microsoft's business communication platform; |
| "Monitoring & Monthly Reporting" | means the Services provided in accordance with paragraph 4.2; |
| "Reactive Technical Support" | means the Services provided in accordance with paragraph 4.3; |
| "Remote Technical Advice" | means the Services provided in accordance with paragraph 4.1; |
| "Security Incident Management" | means the Services provided in accordance with paragraph 4.8; |
| "Service Option" | means the level of service specified in the Order Form as "Essentials", "Enterprise", "Enterprise Plus" or "Bespoke"; |
| "Threat & Vulnerability Management" | means the Services provided in accordance with paragraph 4.7; |
| "Third Party Update" | means an Update to a third party application as specified in the Order Form; |
| "Third Party Update Schedule" | means a process and timescale for the rollout of a Third Party Update to the Update Testing Group and Managed Endpoint Devices, agreed by the Customer and the Company in accordance with paragraph 4.6.1.1; |
| "Update" | means a new version of an operating system or application which adds new features, addresses security vulnerabilities or fixes bugs which can be a Microsoft Quality Update, Microsoft Feature Update, Microsoft Out Of Band Security Update or Third Party Update; |
| "Update Testing Group" | means a subset of the Managed Endpoint Devices which will be used to test a new Update prior to application to all Managed Endpoint Devices; and |
| "Virus Definitions" | means the virus definitions provided by the anti-virus software supplier and as updated from time to time. |

1.2 All other capitalised terms, which are not defined in paragraph 1.1 shall have the meanings stated in the Conditions and/or in Specific Conditions X3 – Standard Operational Services.

## 2 COMMENCEMENT DATE

2.1 The Commencement Date shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of the Microsoft 365 Management Services to the Customer.

## 3 MINIMUM TERM

3.1 The Minimum Term shall be as stated in the Order Form or, if no Minimum Term is specified, twelve (12) calendar months from the Commencement Date.

## 4 DELIVERABLES

4.1 **Remote Technical Advice**

4.1.1 Where specified in the Order Form that the applicable Service Option is "Essentials" or "Enterprise" or where otherwise specified in the Order Form that the Company is providing Remote Technical Advice, the Company will:

4.1.1.1 provide a reactive technical advice line to support the Customer in responding to queries and/or resolving Incidents in respect of the Microsoft 365 Platform;

4.1.1.2 subject to paragraph 4.1.3, allow the Customer to notify the Service Desk of a question or Incident in respect of the Microsoft 365 Platform via telephone and/or web portal, as directed by the Company from time to time;

4.1.1.3 upon receiving a request for Remote Technical Advice:

(a) create a record of the Incident and provide a reference number to the Customer;

(b) categorise the Incident in accordance with the Service Levels set out in Specific Conditions X3 – Standard Operational Services;

(c) attempt to diagnose the Incident initially by telephone to ensure that a suitably qualified engineer responds to the Incident; and

(d) arrange for an appropriately skilled support engineer to call the Customer back within the Incident Response Time.

4.1.1.4 provide assistance via telephone or, where made available by the Customer to the Company, remotely via remote access facilities to the Customer's infrastructure; and

4.1.1.5 where specified in the Order Form that the Remote Technical Advice service is available "Out of Hours", make the Remote Technical Advice service available at any time; otherwise the Company shall make the Remote Technical Advice service available during Support Hours.

4.1.2 The quantity of hours per month that the Company will provide Remote Technical Advice is specified on the Order Form and is subject to the Fair Use Policy.

4.1.3 All Critical Incidents must be logged by the Customer via telephone with the Service Desk.

4.2 **Monitoring & Monthly Reporting**

4.2.1 Where specified in the Order Form that the applicable Service Option is "Enterprise" or "Enterprise Plus"or where otherwise specified in the Order Form that the Company is providing Monitoring & Monthly Reporting, the Company will:

4.2.1.1 monitor the Microsoft 365 Platform in accordance with the Event Management process and notify the Customer by email of alerts raised by this monitoring;

4.2.1.2 use the functionality provided by the Microsoft 365 Platform to create a report showing the End User usage and provide the report to the Customer on a monthly basis unless otherwise specified in the Order Form;

4.2.1.3 use the functionality provided by the Microsoft 365 Platform to create a report showing the asset information for the Managed Endpoint Devices and provide the report to the Customer on a monthly basis unless otherwise specified in the Order Form;

4.2.1.4 use the functionality provided by the Microsoft 365 Platform to create a report showing the license consumption information and provide the report to the Customer on a monthly basis unless otherwise specified in the Order Form;

4.2.1.5 host a call with the Customer and an appropriately skilled engineer:

(a) to review and make recommendations relating to:

(i) the reports provided in 4.2.1.2, 4.2.1.3 and 4.2.1.4; and

(ii) the Microsoft 365 Compliance Centre Dashboard;

(b) on a monthly basis unless otherwise specified in the Order Form.

4.2.2 The call referred to in paragraph 4.2.1.5 will last for no more than one (1) hour unless otherwise specified in the Order Form.

4.2.3 Where the Service Option is "Enterprise Plus", or where Remote Technical Support is included on the Order Form, the Company will, if required, raise an Incident via the Incident Management process for alerts referred to in paragraph 4.2.1.1.

4.3 **Reactive Technical Support**

4.3.1 Where specified in the Order Form that the applicable Service Option is "Enterprise Plus" or where otherwise specified in the Order Form that the Company is providing Reactive Technical Support, the Company will:

4.3.1.1 resolve Incidents in accordance with the Incident Management process;

4.3.1.2 investigate Problems in accordance with the Problem Management process;

4.3.1.3 implement Changes in accordance with the Change Management process; and

4.3.1.4 maintain a configuration management database in relation to the Microsoft 365 Platform and update the stored configuration items on a regular basis.

4.3.2 The Incidents, Problems and Changes referred to in paragraph 4.3.1 will only apply in respect of the following parts of the Microsoft 365 Platform and only if specified as included in the Order Form:

4.3.2.1 Microsoft 365 Core Platform;

4.3.2.2 Microsoft Exchange Online;

4.3.2.3 Microsoft Sharepoint;

4.3.2.4 Microsoft Teams; and

4.3.2.5 Microsoft EMS.

4.4 **Anti-Virus Management**

4.4.1 Where specified in the Order Form that the Company is providing Anti-Virus Management, the Company will:

4.4.1.1 use the Microsoft 365 Platform to manage the anti-virus posture of the Managed Endpoint Devices;

4.4.1.2 perform configuration of the anti-virus software;

4.4.1.3 manage and apply updates to the Virus Definitions:

(a) on a regular basis when released by Microsoft and managed as a Standard Change; and

(b) as advised by Microsoft, where updated Virus Definitions are required to resolve a major security breach or to resolve a security incident, such updates to be managed as an Emergency Change.

4.4.1.4 where a virus is found, notify the End User Service Desk.

4.5 **Microsoft Security & Feature Update Management**

4.5.1 Where specified in the Order Form that the Company is providing Microsoft Security & Feature Update Management, the Company will:

4.5.1.1 agree a subset of Managed Endpoint Devices to form an Update Testing Group which will receive the initial Update;

4.5.1.2 agree a Microsoft Quality Update Schedule with the Customer for Microsoft Quality Updates which:

(a) defines timescales for the rollout of the Microsoft Quality Updates to the Update Testing Group;

(b) defines timescales for the rollout of the Microsoft Quality Updates to the rest of the Managed Endpoint Devices; and

(c) will be agreed in writing by the Customer and the Company during any transition or implementation phase of this Contract or otherwise as soon as reasonably practicable following the Commencement Date;

4.5.1.3 use the Microsoft 365 Platform to automatically implement and manage the deployment of a Microsoft Quality Update:

(a) to Managed Endpoint Devices;

(b) in accordance with the agreed Microsoft Quality Update Schedule; and

(c) in line with any exceptions stated within the Microsoft Quality Update Schedule;

4.5.1.4 in respect of each Microsoft Out Of Band Security Update released by Microsoft:

(a) raise a change for the Customer to review and approve the Microsoft Out Of Band Security Update in accordance with the Change Management process; and

(b) if approved, use the Microsoft 365 Platform to implement and manage the deployment of the Microsoft Out Of Band Security Update to the Managed Endpoint Devices;

4.5.1.5 in respect of each Microsoft Feature Update released by Microsoft:

(a) agree a Microsoft Feature Update Plan with the Customer;

(b) use the Microsoft 365 Platform to implement and manage the deployment of the Microsoft Feature Update to the Update Testing Group in accordance with the Microsoft Feature Update Plan; and

(c) use the Microsoft 365 Platform to implement and manage the deployment of the Microsoft Feature Update to the rest of the Managed Endpoint Devices in accordance with the Microsoft Feature Update Plan;

4.5.1.6 halt the rollout of the Update to Managed Endpoint Devices during testing of the Update Testing Group if requested by the Customer, as soon as reasonably practicable following such request.

4.5.2 The resolution of application or hardware compatibility issues are excluded from Microsoft Security & Feature Update Management.

4.5.3 Any changes to the agreed Microsoft Security & Feature Update Management processes once it is automated may incur additional charges.

4.6 **Application Security Update Management**

4.6.1 Where specified in the Order Form that the Company is providing Application Security Update Management, the Company will:

4.6.1.1 agree a Third Party Update Schedule with the Customer for Third Party Updates which:

(a) defines timescales for the rollout of the Update to the Update Testing Group as specified in paragraph 4.5.1.1;

(b) defines timescales for the rollout of the Update to the rest of the Managed Endpoint Devices; and

(c) will be agreed in writing by the Customer and the Company during any transition or implementation phase of this Contract or otherwise as soon as reasonably practicable following the Commencement Date;

4.6.1.2 review Third Party Updates to identify Updates to be applied in line with the Third Party Update Schedule on a weekly basis unless otherwise stated in the Order Form;

4.6.1.3 use the Microsoft 365 Platform to automatically implement and manage the deployment of a Third Party Update:

(a) to Managed Endpoint Devices;

(b) in accordance with the agreed Third Party Update Schedule; and

(c) in line with any exceptions stated within the Third Party Update Schedule;

4.6.1.4 halt the rollout of the Update to Managed Endpoint Devices during testing of the Update Testing Group if requested by the Customer, as soon as reasonably practicable following such request; and

4.6.1.5 provide Updates only to applications specified on the Order Form.

4.6.2 The resolution of application or hardware compatibility issues are excluded from Application Security Update Management.

4.6.3 Any changes to the agreed Application Security Update Management processes once it is automated may incur additional charges.

4.7 **Threat & Vulnerability Management**

4.7.1 Where specified in the Order Form that the Company is providing Threat & Vulnerability Management, the Company will, on a monthly basis unless otherwise specified in the Order Form, host a call with the Customer and an appropriately skilled engineer to review and make recommendations relating to:

4.7.1.1 the Microsoft EMS Dashboard; and

4.7.1.2 the Microsoft Defender ATP Dashboard.

4.7.2 The call referred to in paragraph 4.7.1 will last for no more than one (1) hour unless otherwise specified in the Order Form.

4.7.3 Forensic investigation and security resolution activites are excluded from Threat & Vulnerability Management.

4.8 **Security Incident Management**

4.8.1 Where specified in the Order Form that the Company is providing Security Incident Management, the Company will investigate each vulnerability reported in the Microsoft Defender ATP Dashboard where the CVSS Score is “critical” or “high”. The Company shall:

4.8.1.1 notify the Customer with recommended actions, or that no further action is necessary;

4.8.1.2 where an Update is recommended, raise a Change to apply an Update to the application as specified in paragraphs 4.5 and 4.6; and

4.8.1.3 investigate each potential security incident reported in the Microsoft Defender ATP Dashboard where the Severity score is “high” or “medium”. The Company shall:

(a) use the Microsoft 365 Platform to investigate the security incident and notify the Customer with recommended actions, or that no further action is necessary; and

(b) raise an Emergency Change via the Change Management process for the use of automated remediation using native Microsoft EMS capability, and implement once approved by the Customer.

4.8.2 Security Incident Management is provided within Support Hours only.

4.8.3 Forensic investigation and security resolution activities are excluded from Security Incident Management.

## 5 CUSTOMER OBLIGATIONS

5.1 The Customer shall:

5.1.1 at all times operate and maintain the Microsoft 365 Platform and Managed Endpoint Devices in a prudent manner and at all times in accordance with the Vendor's recommendations;

5.1.2 ensure timely participation and engagement with the Change Management process;

5.1.3 where the Company is providing Microsoft Security & Feature Update Management and/or Application Security Update Management:

5.1.3.1 approve the requests submitted by the Company in accordance with the Change Management process and will not unreasonably withhold or delay such approval; and

5.1.3.2 inform the Company in a timely manner upon the discovery of an issue relating to the Update Testing Group associated with an Update.

5.1.4 ensure it has paid for all necessary licenses and support for the Microsoft 365 Platform and promptly make available such support to the Company;

5.1.5 ensure it has paid for all necessary licenses and support for any applications included in Application Security Update Management and promptly make available such support to the Company;

5.1.6 accept an invitation from the Company to become linked via a Microsoft Reseller Relationship for the Microsoft 365 Platform and authorise elevated rights access to the Company's technical team;

5.1.7 be responsible for ensuring compliance with the terms of any software licence agreement for the Microsoft 365 Platform or any applications included in Application Security Update Management;

5.1.8 be responsible for maintaining the confidentiality of physical access details to the Managed Endpoint Devices; be liable for all loss and damages arising from unauthorised physical access to or use of the Managed Endpoint Devices; and be responsible for designing and implementing its own security policy within the Customer's operations for preventing such occurrences;

5.1.9 be responsible for maintaining any dependencies required for Microsoft 365 Platform including but not limited to active directory, single sign-on and access management policies;

5.1.10 provide to the Company relevant details of all previously completed triage and diagnostics testing (and results thereof) when raising a request for support in order for the Company to review such request;

5.1.11 where the Microsoft 365 Management Services are to be provided on an existing Microsoft 365 tenancy, provide access to and hand over the tenancy to the Company in a timely fashion and in good working order as reasonably determined by the Company;

5.1.12 remain responsible for the security and firewalls of the Customer's communications links, equipment, software, services and processes unless agreed otherwise in this Contract as being expressly provided by the Company and/or otherwise agreed in writing with the Company; and

5.1.13 take adequate copies of locally-stored data and operating and application software, unless otherwise expressly stated in this Contract as being part of the Microsoft 365 Management Services provided by the Company, such that they may be restored to the Managed Endpoint Devices in the event of loss or corruption.

## 6 EXCLUSIONS

6.1 The following shall be excluded from the Microsoft 365 Management Services:

6.1.1 the cost of any software licenses or hardware. The Company will only deliver particular Microsoft 365 Management Services where the relevant Microsoft 365 license has been purchased by the Customer;

6.1.2 monitoring and alerting on any security incident, unless provided as part of Security Incident Management;

6.1.3 requests for product training or technical consulting;

6.1.4 changes which are deemed by the Company as project work;

6.1.5 support for any operating system build version which is not a Microsoft supported version;

6.1.6 direct interaction with End Users, unless initiated by the Company;

6.1.7 setup or migration of tenancy; and/or

6.1.8 actions related to particular End Users or devices, including but not limited to:

6.1.8.1 reacting to and investigating alerts raised by Microsoft Intune;

6.1.8.2 investigating and removing viruses or other security breaches;

6.1.8.3 fulfiling End User services requests such as remote wipe and remote lock; and

6.1.8.4 resolution of Incidents which only affect a single End User or small group of End Users.

## 7 GENERAL

7.1 The Microsoft 365 Management Services will be provided from the Company's sites.

7.2 All reporting is based on the Company's templated standards and any reports required outside of that standard will incur additional charges.

7.3 Any technical or security advice given in the delivery of the Microsoft 365 Management Services is provided based on the information available at the time and the interpretation of a suitably skilled engineer and as such cannot be guaranteed.

7.4 The Company is not responsible for any data lost or corrupted or rendered inaccessible from the Managed Endpoint Devices or otherwise as a result of security incident, virus outbreak or infection, or caused by misuse of any system or application used on or connected to the Managed Endpoint Devices by End Users or any breach by End Users of any security policy.

7.5 The Company reserves the right to make reasonable adjustments to the Microsoft 365 Management Services if Microsoft changes or removes any functionality which the Company relies on to deliver the Microsoft 365 Management Services.

7.6 The Company will have no liability (whether in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution or otherwise) for any failure to provide the Microsoft 365 Management Services (including failing to meet any Service Level), or to pay any service credit (if applicable), to the extent caused by any interruption or failure of the Microsoft 365 Management Services arising directly or indirectly as a result of any of the following circumstances set out in this paragraph:

7.6.1 any act or omission of the Customer, its agents, representatives or users;

7.6.2 any act or omission of Microsoft or any other relevant third party;

7.6.3 as a result of any delay or failure by the Customer to provide or otherwise comply with the Customer Obligations;

7.6.4 the Customer's failure or delay in complying with the Company's reasonable instructions;

7.6.5 any software other than the Microsoft 365 Platform;

7.6.6 incorrect or unauthorised use of the Microsoft 365 Platform and/or Managed Endpoint Devices;

7.6.7 any unsupported programs used in conjunction with the Microsoft 365 Platform and/or Managed Endpoint Devices; and/or

7.6.8 End Users not powering on and/or not connecting the Managed Endpoint Devices to a suitable network in order to receive any software updates (including Updates and Virus Definitions) in order to maintain compliance to relevant policies;

and the Company reserves the right to levy additional charges to the Customer on a time and materials basis in respect of any additional Services provided by the Company that have been necessitated by such matters.

## 8 CHARGES

8.1 The Charges for the Microsoft 365 Management Services are as identified in the Order Form.

8.2 Unless otherwise provided in the Order Form, the Company will invoice for the Charges for the Microsoft 365 Management Services monthly in advance, with the first invoice issued by the Company on or around the Commencement Date.

## 9 SERVICE LEVELS

The Company will provide Incident Management, Problem Management and Change Management in accordance with the applicable Service Levels set out in Specific Conditions X3 – Standard Operational Services.

## 10 REASONABLE AND FAIR USE

10.1 All Microsoft 365 Management Services are provided on a 'reasonable use' basis, as determined by the Company.

10.2 If, using its reasonable judgement, the Company considers that the use of the Microsoft 365 Management Services by the Customer has consistently or notably exceeded typical usage by other customers, exceeded the Fair Use Policy, or that an individual Request made by the Customer is not reasonable in nature, the Company may take reasonable steps to address the usage pattern or Request. Such steps may include:

10.2.1 remedial work to address the root cause of the issues that are causing overuse of the Microsoft 365 Management Services, such work being chargeable by the Company on a time and materials basis;

10.2.2 revising recurring charges or imposing additional time and materials charges in consideration of the overuse/request;

10.2.3 limiting the Customer's use of the Microsoft 365 Management Services in line with typical customer use; and/or

10.2.4 implementation of or change to a Fair Use Policy relating to the Microsoft 365 Management Services or to a particular element of the Microsoft 365 Management Services.

10.3 All use of the Microsoft 365 Management Services which is covered by a Fair Use Policy will be measured using a three (3) month rolling average.

10.4 The Charges for the Service Options "Essentials" and "Enterprise" will be compared against the quantity of hours purchased.

10.5 The Charges for the Service Option "Enterprise Plus" will be compared against the cost of the effort expanded on delivering the service as follows:

10.5.1 the calculation will be completed on a three month rolling basis;

10.5.2 the Customer will be judged to have exceeded the Fair Use Policy if their usage of the service exceeds 120% of the Charges; and

10.5.3 a resource cost of £30 per hour will be used to determine the usage, which the Company reserves the right to update at its reasonable discretion.