Claranet

Managed Workplace Services

- *Workplace Service Desk*
- *Managed Microsoft 365*
- *Managed Endpoint (Microsoft Intune)*
- *Managed M365 Teams Phone*

Service Description v1.1

claranet | Make modern happen®

Contents

1. Introduction 2
2. Scope of Service Description 2
3. Service Overview 2
4. Service Plans and Components 2
4.1. Workplace Service Desk Component 3
4.2. Managed Microsoft 365 Component 4
4.3. Endpoint Management Service Component 5
4.4. Additional/Optional Features 7
5. Managed Service 8
5.1. Support Levels 8
6. Roles and Responsibilities 10
6.1. Third-Party Systems and Integrations 11
6.2. Third-Party Terms and Conditions 11
6.3. Prerequisites 13
6.4. Service Activation Phase 13
7. Service Levels 0
8. Key Performance Indicators 0
8.1. Endpoint Management KPI 0
9. Delays and Cancellation Terms 0
10. Assumptions and Exceptions 1
11. Terminology 3
12. Appendix 5
12.1. Managed Microsoft 365 Service Plans Datasheet 5
12.2. Managed Endpoint Service Plan Datasheet 9

1. Introduction

This Service Description describes the service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and should be read in conjunction with the terms of the Customer Experience for Managed Services Document ("CXMS") and the Claranet Master Services Agreement ("MSA") set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, all terms used within this document are in accordance with the terms to be found in the CXMS and the MSA.

Claranet provides the following services as part of its Workplace Managed Service ("Service"). The Service components and features are set out below along with the related responsibilities for that Service component/feature.

2. Scope of Service Description

The Customer agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. Any components which are described as optional or additional in this Service Description will be chargeable at additional cost and will need to be purchased by the Customer and an Order Form or Statement of Works will need to be signed by the Customer.
Notwithstanding the foregoing, in the event Claranet completes additional services activities and/or deliverables upon the request or at the direction of the Customer (or the Customer adds users directly on any Customer facing portal), Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed.

3. Service Overview

Claranet Managed Workplace Service delivers a secure, and highly productive Microsoft 365 environment experience. Claranet's comprehensive Service offering includes proactive IT support, security and compliance management, and workplace optimisation. The Service enables organisations to maximise efficiency, enhance collaboration, and drive digital transformation.

4. Service Plans and Components

The Service comprises of three (3) Service Components:

1. Workplace Service Desk.
2. Managed Microsoft 365.
3. Managed Endpoint.

Claranet offers the flexibility to select one, two, or all three components based on the Customer's specific business requirements. This modular approach allows for tailored support and management solutions that can scale with the Customer's organisation's evolving needs.

Alongside the Service Component, Claranet offers three (3) Service Plans: Essential, Plus, and Premium. Claranet can recommend the most appropriate service plan tailored to the Customer's current needs and Microsoft subscription types.

The key differences between these Service Plans are:

Table 1. Service Plans

Category	Essential	Plus	Premium
Support Availability	9am-5pm, Monday to Friday	8am-8pm, Monday to Friday	8am-8pm, Monday to Friday (24x7 support for P1 and P2 tickets)
Range of Supported Features	Basic support and management for Microsoft Business subscriptions as per Section 11.1.	Extended support and management for Microsoft Business Premium and Enterprise subscriptions as per Section 11.1.	Advanced support and management for Microsoft Business and Enterprise subscriptions, guidance and health check as per Section 11.1.

For a more detailed breakdown of each Service Plan associated with Workplace Managed Service components, please refer to Appendix Section 11.

4.1. Workplace Service Desk Component

The Workplace Service Desk is the single point of contact for the Customer to report incidents or submit requests. Where the Customer is already receiving a Claranet-managed service, the Customer's existing Service Desk can also support with its Workplace services.

Table 2. Workplace Service Desk features

Features	Description
Microsoft 365 and Intune Support	The Service Desk provides First-line support for Simple Requests, user-specific issues, and minor incidents.
Third-Party Application Support	The Service Desk may provide first-line support for applications outside the Microsoft 365 environment, subject to an additional fee.
Remote Support	All support is delivered remotely.
ITSM Integration	Claranet can integrate its ITSM system with the Customers upon request for seamless support.

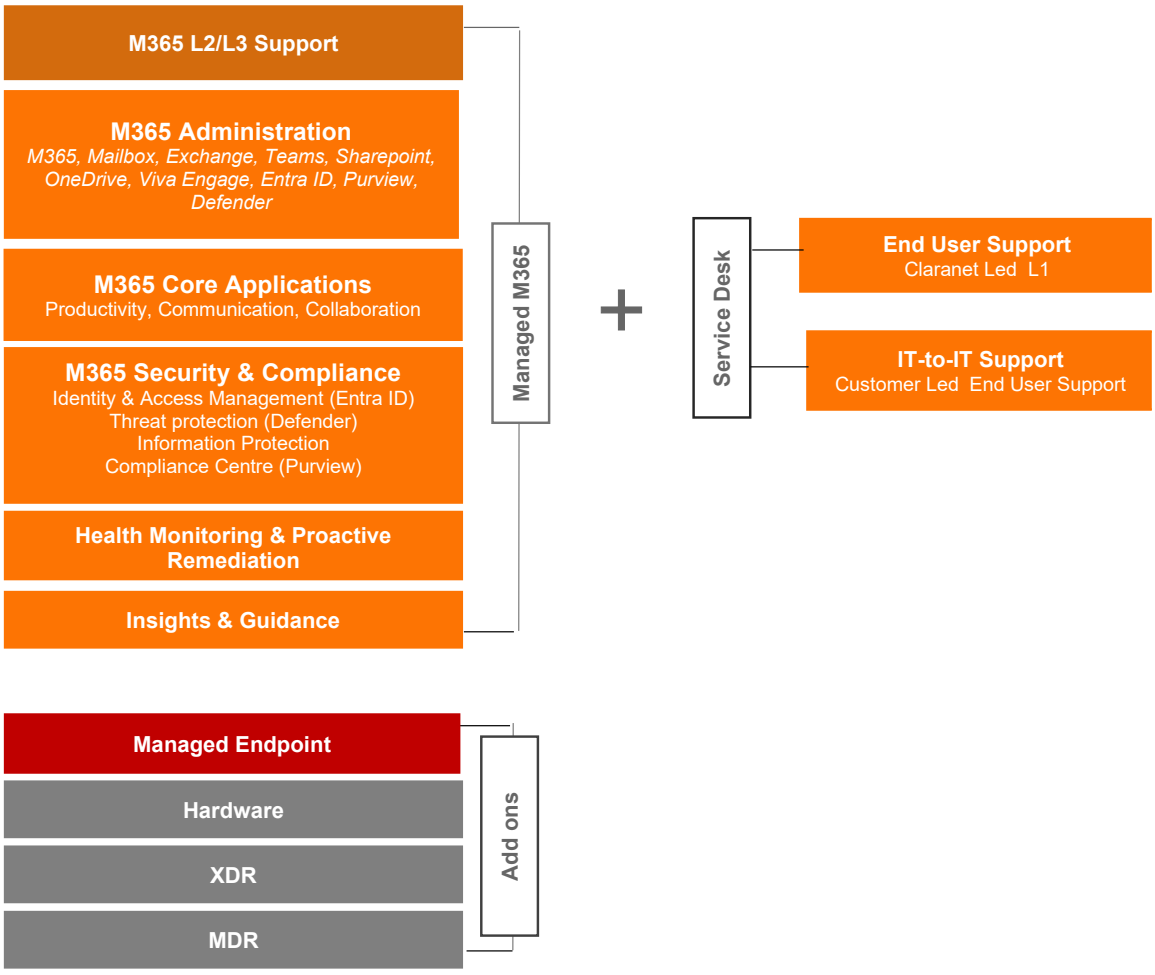
Supported Devices	The Workplace Service Desk supports laptops and desktops.

For comprehensive information regarding case management, ITSM, service reporting, and service levels, please refer to the CXMS Service Description.

4.2. Managed Microsoft 365 Component

The Managed Microsoft 365 Component–involves proactive management of the Microsoft 365 environment, which includes licensing, provisioning, configuration, administration, alerts, and reporting. This Service Component is provided in conjunction with the features available in the Workplace Service Desk Component.

Figure 1. Architecture of Managed Microsoft 365 Service Component



This table highlights the core features as part of the Managed Microsoft 365 Service Component. Detailed information regarding features, service scope, and the breakdown of features included is available in Appendix 11.1.

Table 3. Managed Microsoft365 Service Feature Highlights

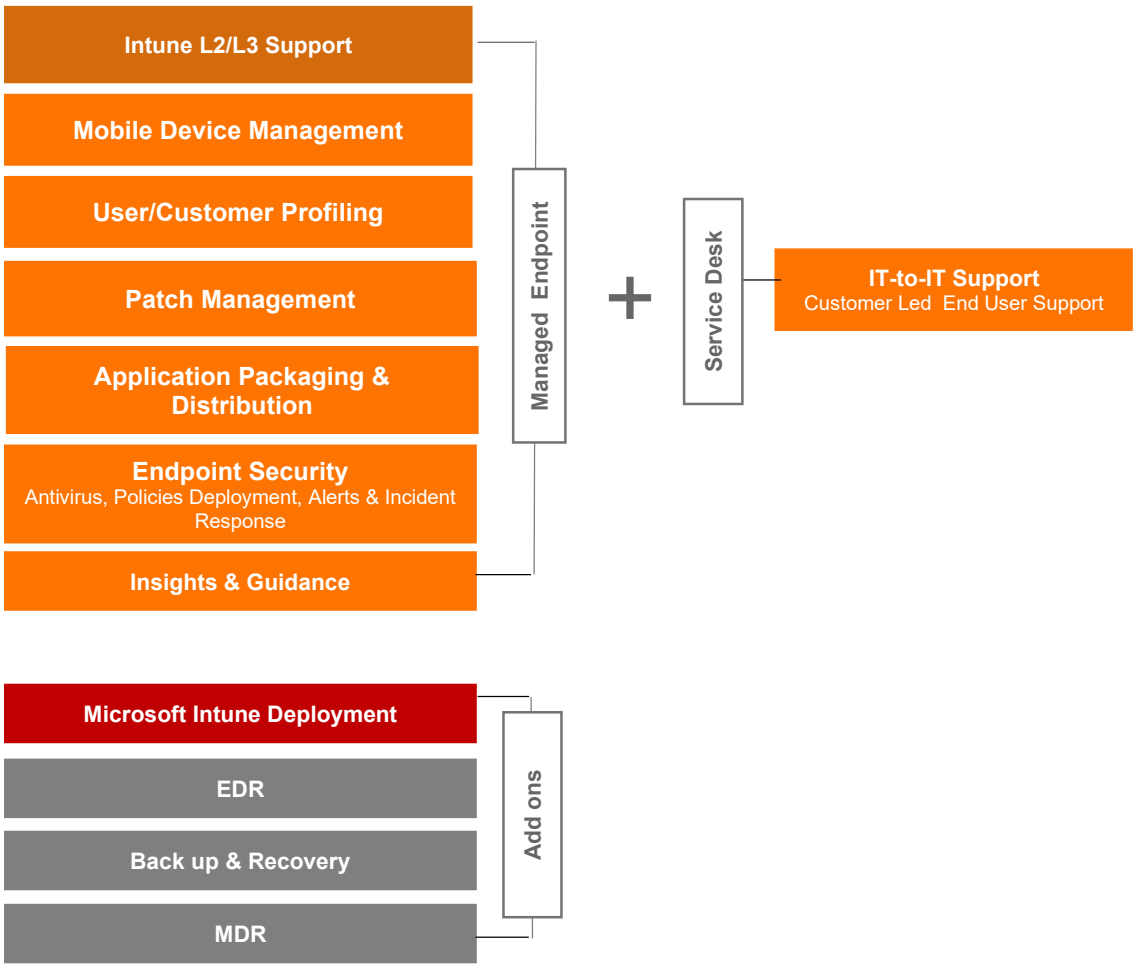
Feature Highlights	Description
Microsoft365 Second and Third Line Support	Claranet will provide Second and Third level support and/or triage for incidents, problems, changes and service requests.
Microsoft365 Administration	Claranet will provide administration of Microsoft 365 admin tools, managing centralised portals and services, such as security and compliance settings, and policy configurations. This includes oversight of key platforms, ensuring seamless operations, optimised licensing, and alerts and reporting of service health and incidents.
Microsoft365 Core Applications (Productivity, Communication, Collaboration)	Claranet will provide the deployment, configuration, security enforcement, integration, performance optimisation, and documentation to support seamless collaboration, data protection, and effective use of Microsoft tools across the organisation.
Microsoft365 Security and Compliance	Claranet provides robust security and compliance management for Microsoft 365, including identity and access control with Entra ID, threat protection with Microsoft Defender, and data governance with Purview. Services include user lifecycle management, policy enforcement, advanced threat detection, DLP, encryption, monitoring, and incident response to ensure data protection, regulatory compliance, and a secure collaboration environment.
Health Monitoring and Proactive Remediation	Claranet ensures optimal performance and availability of Microsoft 365 services through health monitoring, proactive fault remediation, and regular health checks to identify and address potential issues before they impact operations.
Insights and Guidance	Claranet provides actionable insights and strategic guidance through health check reports, advisory services, and M365 strategy reviews to optimise performance, address vulnerabilities, and align Microsoft 365 usage with business goals for maximum ROI.

4.3. Endpoint Management Service Component

This section describes the features of the Endpoint Management Service Component for the Customer's existing infrastructure, including hardware and software.

Please note that the initial hardware provisioning, deployment, retirement, and Microsoft Intune license services are not included in the managed service and must be purchased separately.

Figure 2: Architecture of Managed Endpoint (Microsoft Intune) Service Component



The table below outlines our core capabilities within Managed Endpoint Service Component. Detailed information regarding features, service scope, and the breakdown of features included is available in Appendix 11.2.

Table 4. Managed Endpoint Service Feature Highlights

Feature Highlights	Description
Intune Second and Third Level Support	Claranet will provide Second and Third level support for endpoint devices managed on Microsoft Intune.

Mobile Device Management (“MDM”)	Claranet provides a comprehensive management of Enterprise Policy Management (EPM) and MDM platforms, ensuring secure device enrolment, application management, compliance enforcement, and continuous security monitoring. The Service optimises device performance, enforces corporate policies, and maintains a secure and compliant IT environment across mobile and desktop devices.
User/Customer Profiling	Claranet provides comprehensive asset discovery and inventory management services, ensuring accurate endpoint tracking, compliance, and security. This includes automated asset discovery, inventory updates, regular audits, security assessments, policy enforcement, and profile management to maintain an up-to-date, secure, and compliant IT environment.
Patch Management	Claranet provides end-to-end patch management services, including identifying, testing, planning, and deploying critical updates across Microsoft environments to ensure compatibility, security, and optimal performance. The Service includes proactive customer guidance, troubleshooting, and detailed reporting to maintain system reliability and minimise vulnerabilities.
Application Packaging and Distribution	Claranet provides end-to-end application packaging and distribution services, including assessment, packaging, deployment planning, and execution using Microsoft Intune. The Service includes application rollouts, support of third-party apps, resolves deployment issues, and delivers performance reports to enhance functionality, compliance, and user experience.
Endpoint Security	Claranet provides comprehensive endpoint security management, including anti-virus deployment and monitoring, incident response, and policy development to ensure protection against malware and security threats. The Service focuses on maintaining security compliance, managing vulnerabilities, and implementing robust data governance and identity protection policies across the Microsoft 365 environment.
Insights and Guidance	Claranet provides actionable insights and strategic guidance through health check reports, advisory services, and Endpoint Management strategy reviews to optimise performance, address vulnerabilities, and align Microsoft Intune usage with business goals for maximum ROI.

4.4. Additional/Optional Features

The following feature(s) can be purchased on top of the Subject Plan(s) and will be subject to additional charges:

Table 4. Additional/Optional Features

Feature	Description

Microsoft 365 Subscription and Licensing	Claranet can procure additional licenses for the Customer's Microsoft 365 environment. For more details, please see Claranet's Microsoft 365 Subscription and Licensing Service Description.
Managed M365 Teams Phone	Claranet's Teams Managed M365 Teams Phone Add-On extends our Managed M365 service to include the day-to-day management and administration of your Teams Phone solution, including external (PSTN) calling, numbering, configuration changes, user management, and feature enablement. Service Features: • Management of Teams Phone calling and users features. • Management of Claranet-provided external calling service. • Management of number porting and new provisioning requests. • Change management of Teams Phone and Claranet calling service. • Proactive monitoring of Claranet-provided external calling service. • 24x7x365 support for Teams Phone and Calling service. • Optional add-on to Managed M365 to include Teams Phone.

5. Managed Service

This section pertains to Managed Services and should be read together with the CXMS, which outlines Claranet's core support experience and defines what customers can anticipate from any standard Managed Service solution provided by Claranet. This Section is meant to supplement the CXMS and provide specific details regarding the Service. If there is a conflict between this Section and the CXMS, the terms of this Section will take precedence to the extent of the conflict.

5.1. Support Levels

Table 6. Support Levels

Support Level	Definitions
First Line of Support ("L1")	This is the initial point of contact for end-users.. This level of support handles requests by support analysts with general technical knowledge and basic troubleshooting skills. ("Simple Requests").
Second and Third Level of Support ("L2/L3")	These levels of support handle requests that require experienced technicians and specialists

	to resolve (“Complex Requests”) that First Line support cannot resolve.

The following table will provide examples of what Simple and Complex Requests can include.

Table 7. Simple and Complex Requests Examples

Simple requests (L1: Service Desk)	Complex requests (L2/L3: Managed M365, Managed Endpoint)
Entra ID	
Password Resets & Authentication Issues	**Advanced Licence & Tenant Configuration**
Password reset	Resolving technical discrepancies in licensing assignments or resolving subscription issues
Assisting end users with Multi-Factor Authentication (MFA) setup	Modifying advanced tenant-level settings in Exchange, Teams or Sharepoint
Troubleshooting MFA lockout scenarios	Configure Group License Agreement
Assigning user licences	Analysing sign-in logs for troubleshooting
Creating users and groups	Implement conditional access policies
Exchange	
Troubleshooting email delivery issues	Advanced troubleshooting mail flow issues (SPF/DKIM/DMARC records)
Guiding users in configuring shared mailboxes in Outlook	Configuring email retention policies or litigation holds
Fixing calendar sharing and permission issues	Create advanced transport rules
Delegation access (Shared mailboxes)	Configuration of inbound and outbound connections
Configuration of mailbox forwarding and out-of-office replies	
Other Applications	
Teams and Collaboration issues: Resolving Teams login issues	Security and Access Management: Setting up or troubleshooting custom site collections and permissions structure
Teams and Collaboration issues: Guiding users on joining Teams meetings or setting up a channel	Security and Access Management: Investigating security breaches (compromised accounts flagged by Microsoft Defender)
Basic Troubleshooting: Diagnosing connectivity issues with M365 services (e.g. Outlook not synchronising, Teams not launching etc)	SharePoint/OneDrive: Setting up troubleshooting custom site collections and permissions structures
User onboarding: activating new account, assigning standard licenses profiles based on predefined templates	Teams Governance and Settings: Configuring policies for Teams retention, guest access, or private channels

For more information on the Service Desk features, including case management, incident management, problem management, release management, request fulfilment, service assurance, and change management, please refer to the terms of the Customer Experience for Managed Services Document ("CXMS").

6. Roles and Responsibilities

The Customer, or any appointed third parties, acknowledge and agree to perform their responsibilities. Claranet's delivery, implementation and performance of the Service is dependent upon the timely and effective completion of the Customer's roles and responsibilities and/or as per Claranet's reasonable instructions. If the responsibilities as set out below are not met, and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

Table 8. Roles and Responsibilities

Responsibility	Description
Provide a suitable primary contact for the length of the Service.	To ensure smooth delivery of the Service, the Customer must provide Claranet with a primary contact with the relevant knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service Description and/or the SOW.
Access to support, key staff and stakeholders.	The Customer must provide key staff and stakeholders, both internal and external (where relevant), who are available for engineer visits, meetings, and/or workshops. The Customer will provide the necessary access to support and relevant personnel. However, the Customer will be responsible for ensuring all communications to all key or relevant Customer-managed stakeholders regarding the Service for the duration, including any technical change and/or approval required.
Provide a safe and suitable working environment.	Where Claranet employees are required to attend Customer and/or third-party premises, the Customer must ensure that Claranet employees are provided with a safe and suitable working environment.
Provide information required by Claranet.	The Customer shall provide any information requested in the format specified by Claranet within five (5) working days, unless agreed otherwise in writing.
Responding to project requests by Claranet.	The Customer shall respond to any project-related request made by Claranet within five (5) working days. Unless agreed otherwise in writing.

Reasonable and timely cooperation	The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet.
Notifications regarding maintenance	The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance is scanning, verifying, and identifying vulnerabilities within the Customer's Assets.
Changes to information	The Customer will ensure that technical details are kept up to date by submitting to Claranet to update the relevant details.

6.1. Third-Party Systems and Integrations

Alongside the Service, the Customer may gain or require access to third party systems or portals, and the details of such systems and the level of access will be confirmed outside of this Service Description. Claranet shall not be liable and cannot guarantee uninterrupted access to these systems.

Note: The Customer's access may vary and may be affected by causes outside of Claranet's control, such as but not limited to, maintenance, updates or patching of third-party systems by third parties or the Customer's intentional/unintentional changes to the scope, consumption or size of their Service. This may result in downtime and paused SLAs, as well as additional charges/Fees, including but not limited to, over usage charges.

6.2. Third-Party Terms and Conditions

As part of the Agreement with Claranet, the Customer's Service will be provided in accordance with the Terms of Service between Microsoft and the Customer in relation to Customer's use of the Microsoft software as part of the solution or Service provided by Claranet.

The Customer agrees to and confirms that the it has read and understand that the Customer is bound by the Microsoft Terms of Service set out herein in relation to the Services/software, which can be found at: **Licensing Documents (microsoft.com)**

The Customer acknowledges and agrees that in taking this Service from Claranet that the Customer has been given access to, has read and agree to the Microsoft Support Terms that apply to Customer's use of the Services/software as part of the Service or solution that Claranet are providing under this

Service Description, which can be found here: **Microsoft 365 and Office 365 service descriptions - Service Descriptions | Microsoft Learn**

Claranet reserves the right to amend this Service Description in accordance with any changes implemented by Microsoft.

6.3. Prerequisites

Prior to Claranet commencing the Services, the Customer must complete the specified prerequisite activities to ensure successful delivery. Failure to meet these prerequisites may adversely affect service delivery, potentially preventing Claranet from fulfilling its obligations and possibly necessitating modifications through a Change Request Form to address any impacts.

The table below outlines the required prerequisite activities for guidance purposes. Based on the project's complexity, these activities may be expanded.

Table 9. Prerequisites

Prerequisites
The managed service assumes that the necessary infrastructure, such as Microsoft Intune licences, is in place, fully deployed, and properly configured.
To ensure a thorough assessment, the Customer is required to provide Claranet with the necessary admin access to the following platforms: • **Microsoft 365:** Full global administrative access to Microsoft 365 services. • **Azure AD**: Administrative access to Azure Active Directory. • **Intune**: Administrative access to Microsoft Intune.
Additionally, the Customer will engage in the following sessions: • **Service Tiers and Design Discussion:** Participate in a detailed session to discuss the various service tiers and the overall service design. This session will help align expectations and clarify the scope of services. • **Assessment Findings Review:** Attend a session to review the assessment findings. This session will highlight key insights and identify quick wins that can be implemented to enhance the service. • **Service Model and Stakeholder Roles Review:** Attend a session to review the proposed service model and the roles of various stakeholders. This will ensure that all parties know their responsibilities and the overall service structure. • **Final Service Model Approval:** Review and approve the final service model and setup. This step is crucial to ensure that the service is tailored to meet the Customer's specific needs and requirements.

Note: In the event a prerequisite activity is not completed, the delivery of Service may be delayed, quality of Service may be impacted and/or additional costs may be incurred to deliver the Services. In addition, the Service shall not be subject to the SLAs or Service Credits (if applicable) and shall be provided on a reasonable endeavours basis until the above activities are completed.

6.4. Service Activation Phase

In implementing the Service, Claranet will carry out the following activities with the Customer:

Table 10. Service Activation Phases and Tasks

Phase	Tasks

Assessment Phase	• Evaluate existing environments and processes.
	• Identify compliance gaps with standards and best practices.
	• Review asset lifecycle management.
	• Assess security measures and compliance.
	• Evaluate user profile and patch management.
	• Analyse software distribution methods.
	• Identify recommendations for the Customer's environment.
	  ○ These recommendations will be categorised into continuous improvement initiatives, which will be managed during the service operation, and blockers, which must be resolved before service activation can continue.
	• Any identified blockers must be addressed before the managed service can commence.
	  ○ Claranet includes up to 16 hours of engineering time to resolve minor blockers within the scope of the initial engagement.
	  ○ Should the resolution of blockers require additional time or resources beyond this allocation, these will either be subject to additional charges or will need to be resolved by the customer prior to proceeding with the managed services onboarding.

Remediation Plan Development (if needed)	• Develop a remediation plan based on assessment. • Prioritise tasks by risk and impact. • Define timelines and responsibilities. • Recommend enhancements for compliance.
Setup of Support and Administrative Services	• Define a support structure (RACI matrix). • Establish service management and incident handling processes. • Implement tools for service delivery. • Train personnel on new processes and tools.

Phase	Tasks

Knowledge Transfer and Documentation	• Conduct knowledge transfer sessions.
	• Create documentation, including:
	  • Assessment findings;
	  • Remediation plan;
	  • Support and administrative processes.

Endpoint Management – Software Identification for Packaging and Distribution	• Review applications, including operating systems, Microsoft apps, and browsers, to ensure appropriate packaging for deployment. • The Plus package supports up to 5 additional named applications; the Premium package supports up to 10. Java and SGBD are not supported.
Intune Service Activation vs Service Deployment	• Includes only the enablement of the managed service and does not encompass platform deployment or configuration. ○ If assistance with Microsoft Intune deployment or configuration is required, this will be treated as a separate project and subject to additional charges.

7. Service Levels

This section details Service Levels that differ from or add to the standard CXMS.

The following Service Level Agreement ("SLA") shall only apply where the Customer has more than 20 tickets per month, and where a Customer has less than 20 tickets per month, the following SLAs shall not apply.

The SLAs will be calculated per month and the Customer shall receive a monthly report for SLA and Performance Management.

1. Service Level Agreements

Table 11. Service Level Agreements

Category	P1: High	P2: Normal	P3: Low
Definition	Severe impact on business operations, where multiple users or key Endpoints are completely unavailable or unusable; 50% or more of the total devices in the environment are impacted	Significant but limited impact on business operations. Some users or Endpoints are affected, but core functions remain operational; between 20% and 50% of the total devices in the environment are impacted	Minor issues with low or no direct impact on business operations. Often involves a single user or a small number of non-critical devices; less than 20% of the total devices in the environment are impacted
Service Desk SLA – Incident Response (INC)			
Response Time	90% of Incident Tickets will receive a response within 3 hours	90% of Incident Tickets will receive a response within 4 hours	90% of Incident Tickets will receive a response within 4 hours
Resolution Time	90% Incident Tickets will be resolved within 8 hours	90% of Incident Tickets will be resolved within 12 hours	90% of Incident Tickets will be resolved within the NBD*
Service Desk SLA – Service Response (SR)			
Response Time	90% Service Tickets will receive a response within 4 hours	90% of Service Tickets will receive a response within 6 hours	90% of Service Tickets will receive a response within 6 hours

Resolution Time	90% of Service Tickets will be resolved within 8 hours	90% Service Tickets will be resolved within 12 hours	+ 90% of Service Tickets will be resolved within the NBD*
Managed M365 and Endpoint SLA – Incident Response (INC)			
Response Time	90% of Incident Tickets will receive a response within 4 hours	90% of Incident Tickets will receive a response within 8 hours	90% of Incident Tickets will receive a response within 12 hours
Resolution Time	90% of Incident Tickets will be resolved within 4 hours	90% of Incident Tickets will be resolved within 8 hours	90% of Incident Tickets will be resolved within the NBD*
Managed M365 and Endpoint SLA – Service Response (SR)			
Response Time	90% of Service Tickets will receive a response within 4 hours	90% of Service Tickets will receive a response within 8 hours	90% of Service Tickets will receive a response within NBD
Resolution Time	90% of Service Tickets will be resolved within 8 hours	90% of Service Tickets will be resolved within the NBD*	90% of Service Tickets will be resolved within two business days of Ticket creation
Response Time Service Credit			
Response SLA Service credit	Up to 10% of the monthly service fee	Up to 5% of the monthly service fee	N/A

*-NBD (next business day)

In the event that a Customer submits a valid claim that Claranet did not meet its Service Level Agreement, Claranet will verify and if verified, shall raise a credit note to the Customer's account that shall be applied to the next invoice in its billing cycle. Such Service Credits will be calculated based on the percentage of SLAs not met per Service Component and will be based on the applicable percentage of the monthly Fee. The maximum amount of Service Credit a Customer can receive in each calendar month relating to this Agreement is limited to 10% of the Monthly Fee for the affected Service. Such Service Credits are pre-agreed liquidated damages and, unless stated otherwise in the Agreement, such Service Credits will constitute the Customer's sole and exclusive remedy with respect to the breach of SLAs.

8. Key Performance Indicators

8.1. Endpoint Management KPI

The table below provides an overview of service availability periods and key performance indicators (KPIs) for the Endpoint Management Service Component.

Table 11. Endpoint Management KPIs

Service KPIs	Essential	Plus	Premium
Operating System Patch Installation	90% of Endpoints updated within ten (10) business days	90% of Endpoints updated within ten (10) business days	95% of Endpoints updated within ten (10) business days
Security Patch Installation	90% of Endpoints updated within ten (10) business days	90% of Endpoints updated within ten (10) business days	95% of Endpoints updated within ten (10) business days
Application Availability	-	Five (5) business days	Five (5) business days
Provision of Certified Standard Image	-	-	Ten (10) business days

9. Delays and Cancellation Terms

1. Professional Services must be used within 6 months from the date of Customer's signature of the Order Form and at expiry of this period, Claranet may invoice the full remaining Professional Services Fees and the Customer will pay those Fees in accordance with the Agreement. Thereafter, the Customer will have a further 6 months to use those remaining Professional Services, after which they will expire on such date if unused. Unless agreed otherwise, Professional Services are non-refundable.
2. The Customer agrees and acknowledges that Claranet will estimate the time required to complete the Services and that additional days of Professional Services may be required to complete the Services. Claranet shall notify the Customer where it determines in good faith additional days are required to complete the Services and such additional days may then be authorised by the Customer in accordance with Change Request Form or an additional Order Form.
3. Notwithstanding the above, if the project is delayed or put on hold by the Customer (expressly or impliedly) after the date of signature for a cumulative period of:

    a) 1 (one) month, the project status will be reviewed for viability;
    b) 2 (two) months, the project status and viability will be reviewed, the project will be marked as "at-risk"; and

c) 3 (three) months, Claranet reserves the right to cancel the project and invoice the Customer for the greater of (a) any Services delivered up to the point of such cancellation, or (b) the amount payable pursuant to Clause 4.2 of the MSA.

4. If the Customer postpones or cancels a booking (e.g. a workshop, meeting or a call) at short notice, then the following will be charged by Claranet, depending on the amount of notice given:

Table 12. Postponement or Cancellation Fees

Notice for Postponement or Cancellation	Postponement or Cancellation Fee
Less than 15 working days but greater than 10 working days	50% of the Fees associated to the booking
Less than 10 working days but greater than 5 working days	75% of the Fees associated to the booking
Less than 5 working days	100% of the Fees associated to the booking

5. If the Customer seeks to cancel a Service/s before the expiry of the Initial Term or Renewal Term, Claranet will automatically invoice and the Customer shall pay for cancellation charges equivalent to the total Fees that would otherwise have otherwise be payable for the remainder of the Initial Term or Renewal Term of the respective Service/s, unless agreed otherwise.

6. Once the cancellation has been processed by Claranet, the Customer shall follow Claranet's reasonable instructions to decommission any hardware and to cease access to relevant systems that the Customer received as part of the Service.

10. Assumptions and Exceptions

Where relevant and to the extent any Service Levels set out herein are impacted by the below, Service Credits will not apply as a result.

1. It is assumed that where required as part of the Service, access to the Customer's IT infrastructure is quickly established and retained for the duration of the Service. Any issues relating to access and permissions may result in work being halted or delayed until such access is resolved, or cause failures in delivery because Claranet personnel are unable to access the Customer's relevant sites.

2. Where software licences are not provided as part of the Service, it is the Customer's responsibility to ensure they have the appropriate subscriptions and licences as required to benefit from the Service. The costs of such licences and subscriptions are not included in the price of the Service as set out in this Service Description unless otherwise provided in the Agreement.

3. Global Service Desk operates a fair usage policy. If ticket volumes are considered to exceed this threshold, Claranet reserves the right to apply additional service fees to address the increased demand.

4. Claranet is not responsible for any failure of any component for which Claranet has no control over, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer.

5. Claranet excludes responsibility for meeting any Service Levels to the extent that meeting the Service Level is affected by the following exceptions hereunder and Service Credits will, therefore, not be paid if the outage occurs from such exceptions:

    a. if the Customer is in default under the Agreement;

    b. in the event that the Service is unavailable due to any component, event or situation not wholly within the control of Claranet, including but not limited to a failure of a component that Claranet is not responsible, electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;

    c. in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;

    d. in the event that the Service is disrupted or unavailable due to viruses, unauthorised users or hackers;

    e. in the event that the Service is unavailable due to changes initiated by the Customer, whether implemented by the Customer or by Claranet on its behalf;

    f. in the event that the Service is unavailable as a result of the Customer exceeding system capacity;

    g. in the event that the Service is unavailable due to viruses, not arising from the failure or breach of Claranet or Claranet's Service;

    h. in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;

    i. in the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;

    j. in the event that the Service is unavailable due to Customer's third party contractors or vendors or anyone instructed by the Customer gaining access to Claranet's network, control panel or to the Customer's website at its request;

    k. in the event that the Service is unavailable due to a force majeure event;

    l. in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;

    m. in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct or of others authorised by the Customer to use the Services provided by Claranet;

n. in the event that the Service is unavailable due to any failure of local access facilities provided by the Customer;

o. in the event that the Service is unavailable due to any failures that cannot be corrected because the Customer are inaccessible or because Claranet personnel are unable to access the Customer's relevant sites; and

p. any failure of local access facilities provided by the Customer.

11.Terminology

Unless otherwise specified, capitalised terms used in this Service Description shall bear the same meanings as those used in the Master Service Agreement, unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

Table 13. Terminology

Terms	Definition
Customer Experience for Managed Services (CXMS) Document	The CXMS document provides a framework for Claranet's core managed support experience and describes what a customer can expect from any standard Managed Service provided by Claranet. It outlines the responsibilities, how to log and escalate cases, how SLA targets are prioritised, set, and achieved, etc.
SLA (Service Level Agreement)	An agreement defining the expected level of service from a provider, including response and resolution times.
Pre-Requisites	Activities that must be completed by the Customer before Claranet can commence the services.
Service Credits	Pre-agreed liquidated damages that a Customer can receive if Claranet does not meet its Service Level Agreement.
Patch/Patching	A patch is a set of software changes or updates that are applied to an existing software program or system to fix bugs, address security vulnerabilities, or improve functionality, usability, or performance.
Incident Management	This process involves identifying, analysing, and resolving incidents that disrupt or degrade the quality of IT services. The primary goal is to restore normal service operation as quickly as possible
Problem Management	This process focuses on identifying and managing the root causes of incidents to prevent their recurrence. It involves diagnosing the underlying problems and implementing permanent solutions.

Change Management	This process involves managing changes to the IT environment to minimise the impact on services. It ensures that changes are implemented in a controlled and systematic manner.
Configuration Management	This process involves maintaining information about configuration items required to deliver an IT service. It ensures that the configuration of systems and services is known and documented.
CSAT (Customer Satisfaction)	Customer Satisfaction Score, is a metric used to gauge how satisfied customers are with a company's products, services, or overall experience. It is typically measured through customer feedback surveys.
Image Management	The process of creating and deploying standardised operating system images to devices. This involves capturing a "snapshot" of a configured system, including the operating system, applications, and settings.
Golden Image	A pre-configured template that includes an operating system, applications, and software configurations. It is used to streamline the deployment of new devices, ensuring consistency and reducing setup time.
Configuration Management Database (CMDB)	A centralised repository that stores information about the configuration items (CIs) in an IT environment. This includes details about hardware, software, network devices, and documentation.
Service KPIs (Key Performance Indicators)	Metrics used to evaluate the effectiveness and efficiency of a service. They help in measuring how well a service is performing against its objectives.
XDR (Extended Detection and Response)	A cybersecurity solution that integrates multiple security tools and data sources into a single platform to detect, investigate, and respond to threats across an organisation's entire digital environment.
MDR (Managed Detection and Response)	A cybersecurity service that combines advanced threat detection technologies with expert human analysis to proactively identify, investigate, and respond to security threats.
EDR (Endpoint Detection and Response)	A cybersecurity solution designed to monitor, detect, and respond to threats on endpoints, such as laptops, desktops, and servers.
Apps (Applications)	Software programs designed to perform specific tasks or functions for users, ranging from productivity tools like word processors to communication, collaboration and other specialised business solutions.
Simple Requests	Requests that do not require technical or specialist knowledge to resolve.
Complex Requests	Requests that require experienced technicians and specialists to resolve

ITSM	ITSM (IT Service Management): A structured approach to designing, delivering, managing, and improving IT services within an organisation.
Endpoint Management	The practice of centrally managing and securing devices such as laptops, desktops, mobile phones, and tablets to ensure compliance, security, and optimal performance.

12. Appendix

12.1. Managed Microsoft 365 Service Plans Datasheet

The table below outlines the detailed scope of the three Service plans:

Table 14. Managed Microsoft 365 Service Plans Scope Details

Features	ESSENTIAL	PLUS	PREMIUM
Tools and Portals			
Microsoft 365 Admin Center - *centralised management of all M365 services*	●	●	●
M365 Mailbox Management - *provisioning, size limits, compliance settings*	●	●	●
Exchange Admin Center - *email routing, retention policies, security configurations*		●	●
Teams Admin Center - *settings, policies, user permissions*		●	●
SharePoint/OneDrive Admin Center - *storage quotas, permissions, data-sharing policies*		●	●
Viva Engage Admin Center - *manage platform, users, community, Groups, policy & compliance*		●	●
Entra ID Portal - *oversee identity, access management, controlling user authentication, SSO, and security policies*		●	●
Microsoft Purview Compliance Portal - *administer security settings and monitor threats*		●	●
Microsoft Defender Portal - *administer security settings and monitor threats*		●	●
Administration Activities			
Policy Management - *security, compliance, data retention*			●
License Provisioning - *allocation, optimisation*	●	●	●
User Management - *creation, modification, deletion*	●	●	●
Monitoring and Alerts - *service health, incident detection*		●	●
MANAGEMENT			
Subscription Management Portal - *oversee subscription status, track renewals, and manage payment information*	●	●	●
Subscription Guidance - *best practices and recommendations, insights into potential upgrades or changes to subscription plans*			●
User Management*			

Features	ESSENTIAL	PLUS	PREMIUM
M365 License Provisioning	●	●	●
M365 User Management - *user account creation, modification, deletion, role-based access control*	●	●	●
Microsoft Tools Management	**7 Apps** Word, Excel, PowerPoint, Outlook, Teams, OneDrive, Exchange Online	**10 Apps** Word, Excel, PowerPoint, Outlook, Planner, OneNote, Forms, Teams, OneDrive, Exchange Online	**12 Apps** Word, Excel, PowerPoint, Outlook, Planner, OneNote, Forms, Teams, OneDrive, **SharePoint,** Exchange Online, **Viva**
License Management - *licenses assign to users, monitor usage, renewals, and compliance*	●	●	●
Deployment and Installation - *deploy applications to users' devices, ensure proper installation, configuration, compatibility*	●	●	●
Configuration and Customisation - *settings, preferences for applications, customise features, templates, add-ins*	●	●	●
User Provisioning and Access Management to collaboration and communication Apps - *access permissions based on users' roles*	●	●	●
Security and Compliance - *implement security measures to protect data, documents, enforce security policies, encryption, access controls*	●	●	●
Integration and Collaboration - *real-time co-authoring, version control, integration with cloud storage services, other tools, platforms, systems*	●	●	●
Email Management and Archiving - *manage email accounts, distribution lists, mailboxes in Exchange Online, implement email archiving and retention policies (subject to archiving licencing)*	●	●	●
***In*teroperability** - *data exchange between communication/collaboration solutions and other cloud services, on-premises applications, external platforms*	●	●	●
Version Control and Updates - *monitor and manage software updates, patches, version upgrades for Microsoft Office applications, deploy updates*	●	●	●
Documentation - *management of policies, procedures, best practices for using Microsoft Office applications*	●	●	●
***P*erformance Monitoring and Optimisation** - *identify opportunities for improvement, analyse usage patterns, user feedback, and performance metrics*			●
Identity and Access Management - Microsoft Entra ID			
User Lifecycle Management - *provision, manage, and deactivate user accounts, creating new user accounts, assigning appropriate permissions/roles, group memberships*	●	●	●
Identity Verification and Authentication - *implement, monitor, support, configure authentication mechanisms: passwords, multi-factor authentication (MFA)*	●	●	●
Access Control and Authorisation - *define, monitor, support access policies/permissions*		●	●

Features	ESSENTIAL	PLUS	PREMIUM
Single Sign-On (SSO) - *enable SSO capabilities, integrate Entra ID with SaaS apps, on-premises applications, custom-built apps*		●	●
Identity Federation and Directory Synchronisation - *establish trust Entra ID v's external identity providers, implement directory synchronisation tools*		●	●
Security and Threat Detection - *implement, monitor, support security measures to protect Entra ID identities, detect, mitigate identity-based risks*		●	●
Identity Governance and Compliance - *enforce policies to ensure compliance, implement access reviews, entitlement management, and privileged identity management*		●	●
Monitoring and Auditing - *user activities, access requests, authentication events within Entra ID, utilise Entra ID logs, audit reports, security monitoring tools*		●	●
Microsoft Defender			
Threat Protection - *configure/manage anti-malware policies, monitor/respond to threat detection alerts*		●	●
Email Protection - *implement/manage email filtering policies, configure anti-phishing policies*		●	●
Data Loss Prevention (DLP) - *define/reinforce DLP policies, monitor/analyse data usage and sharing activities*			●
Advanced Threat Protection (ATP) - *enable/configure ATP features such as Safe Links, Safe Attachments, and spoof intelligence, investigate/ remediate ATP alerts and incidents*			●
Security Analytics and Reporting - *utilise security analytics tools to gain insights into security threats, trends, vulnerabilities, generate and review security reports/ audit logs*			●
Incident Response and Remediation - *develop procedures and playbooks to respond to security incidents, breaches, and data leaks, coordinate with incident response teams, IT admins*			●
Policy Configuration and Optimisation - *configure security policies to align with organisational security& compliance requirements, update security policies based on evolving threats, industry trends*			●
Microsoft Information Protection (Purview)			
Policy Creation and Enforcement - *develop policies on sensitive information, enforce to automatically classify/ label documents, emails; apply encryption, access restrictions, retention policies*		●	●
Classification and Labelling - *define classification labels and apply them to documents, emails, and other data assets, implement automatic classification and labelling*			●
Encryption and Rights Management - *utilise technologies to protect sensitive data at rest and in transit, apply encryption to files, emails, communications*		●	●
Data Loss Prevention (DLP) - *implement DLP policies, configure rules to monitor, block, or restrict the transmission of sensitive*			●
Access Control and Authentication		●	●

Features	ESSENTIAL	PLUS	PREMIUM
- *implement access control mechanisms, utilise identity and access management solutions (Entra ID)*			
Monitoring and Auditing - *usage and access patterns of sensitive data, utilise logging, auditing, reporting capabilities to track data access, sharing activities, and compliance*		●	●
Compliance and Reporting - *ensure compliance, generate reports, conduct risk assessments, maintain documentation*		●	●
Incident Response and Remediation - *establish procedures, develop incident response plans, conduct drills/simulations, collaborate with stakeholders*			●
Health Monitoring and Proactive Remediation			
Proactive Remediation of Faults - *monitor the environment for potential faults, implement automated workflows to resolve identified faults*		●	●
Proactive Remediation of Health Check Results - *conduct health checks of the M365 services, analyse results to identify areas for improvement and take necessary actions to enhance service health*			●
Insights & Guidance			
Heath Check Reports - *regularly reports, identification potential areas for improvement*		● Annual	● Annual
Heath Check Advisory - *recommendations to identified issues, implementation of the best practices in governance, security, compliance*		● Annual	● Annual
Microsoft 365 Strategy Review - *M365 usage assessment, identification of gaps, recommendations to maximise ROI*			● Annual
WMS Technical Account Management			● 4h, monthly

Note: More details on each feature support scope are available on request

- **- Additional users only**

12.2. Managed Endpoint Service Plan Datasheet

The table below details the scope of the three tiers of support provided under the Endpoint Management Service Component:

Table 15. Managed Endpoint Service Plans Scope Details

Features	ESSENTIAL	PLUS	PREMIUM
Asset Discovery & Inventory			
Conduct Discovery - *automated tools to gather data on all deployed endpoints*	●	●	●
Update Asset Inventory - *ensure up to date asset inventory in the Configuration Management Database (CMDB)*	●	●	●
Validate Asset Information - *audit the inventory on the current state of endpoints and resolve discrepancies*	● Annual	● Annual	● Bi-Annual
Compliance and Security Assessment			
Perform Compliance Checks - *assess the endpoints for compliance with policies, security requirements, regulations*	Onboarding/ Annual	Onboarding/ Annual	Onboarding/ Bi- Annual
Evaluate Security Posture - *conduct security assessments to identify vulnerabilities, outdated software, compliance gaps*	Onboarding/ Annual	Onboarding/ Annual	Onboarding/ Bi- Annual
Policy Enforcement - *ensure that security policies are enforced on all endpoints, inc. anti-virus, encryption, access controls*	●	●	●
User Profile and Policy Management			
Profile Evaluation - *assess user profiles to ensure they meet business/user needs*	● Annual	● Annual	● Bi-Annual
Policy Updates - *review and update endpoint management policies to reflect changes*	● Annual	● Annual	● Bi-Annual
Patch Management			
Management Tool - Microsoft Intune	●	●	●
- *Identifying important patches*	Operating System Microsoft Applications Additional Browser (e.g. Google Chrome)	Operating System Microsoft Applications Additional Browser (e.g. Google Chrome) up to 5 Applications (Java, SGBD, not included)	Operating System Microsoft Applications Additional Browser (e.g. Google Chrome) up to 10 Applications (Java, SGBD not included)
- *Proactive patches information and guidance to Customers*			
- *Patch Requirements Gathering*			
- *Patch Deployment Tests & Acceptance*			
- *Plan Patch Deployment*			
- *Troubleshooting deployment issues*			
- *Reports on deployment status*			
Application Packaging & Distribution		● up to 5 Applications	● up to 10 Applications
- *Application Assessment, Packaging, Deployment, Custom scripting, Troubleshooting, 3rd-party Apps Support, Status Reports*		●	●
Endpoint Security Management			
- *Antivirus Management*	Microsoft Defender	Microsoft Defender	Microsoft Defender

Features	ESSENTIAL	PLUS	PREMIUM
- *Antivirus Software Deployment*	Subject to Licensing	Subject to Licensing	●
- *AV Defender Platform Management, performance monitoring, updates and patches*	●	●	●
- *Incident Response*	**Basic** · Alert Qualification (validity and priority) · Basic Remediation (e.g. quarantining files or restarting affected systems, to resolve low-risk incidents)	**Standard** · Alert Qualification (validity and priority) · Detailed Remediation (e.g.malware removal, system restoration, and applying necessary patches) · Documentation (Record incident details, actions taken, and resolutions for future reference)	**Advanced** · Comprehensive Alert Analysis (severity and impact) · Detailed Remediation (e.g.malware removal, system restoration, and applying necessary patches) · Proactive Remediation (implementing preventive measures) · Reporting and Recommendations (Record incident details, actions taken, and resolutions for future reference; provide recommendations for improving security posture and incident response capabilities)
Policy Development and Compliance Framework			
Microsoft Defender for Endpoint			
- *create and/or update/ manage security policies, procedures*	●	●	●
- *Develop/manage policies for endpoint hardening and vulnerability management*			●
Microsoft Purview			
- *define/manage compliance policies and procedures*			●
- *develop, implement/manage policies for data governance, retention, DLP*			●
Microsoft Information Protection (MIP)			
- *Develop/manage data classification and labeling policies*			●
Microsoft Entra ID			
- *establish/ manage policies for identity and access management (MFA, Conditional)*	●	●	●
- *create/ manage identity protection policies to monitor/mitigate risks*			●
- *develop/manage policies for role-based access control (RBAC) and least privilege access.*			●
Defender for Cloud Apps			
- *Develop/manage governance policies for cloud app usage, incl. data sharing, access controls*			●
Monitoring and Incident Response	● Annual	● Bi-Annual	● Quarter
Insights and Guidance			
- *Health check reports*	● Annual	● Bi-Annual	● Quarterly
- *Microsoft Security Adoption Score*	● Annual	● Bi-Annual	● Quarterly

Features	ESSENTIAL	PLUS	PREMIUM
- *Health Check Advisory & Remediation Plan*		● Annual	● Bi-Annual
- *Endpoint Management Strategy Review*		● Annual	● Annual
- *Advisory & Consulting Services (Technical Account Mngt/ Customer Success Mngt)*			● 4h monthly
Service Management			
- *Reporting & Analytics*		●	●
- *SLA & Performance Management*	● Monthly	● Monthly	● Monthly

Note: More details on the support scope of each feature are available upon request.