Master Services Agreement:

Annexure I: Service Schedule: M365 Security and Compliance V10-13

This Service Schedule for **M365 Security and Compliance V10-13** (the "Service") supersedes all previously signed or incorporated versions of the Service Schedules for M365 Security and Compliance (if any). It forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule, the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. **"CIS"** means Centre for Internet Security.

1.2. "**CIS Benchmarks**" means a collection of best practices for securely configuring IT systems, software, networks, and cloud infrastructure[1]. They are published by the Centre for Internet Security (CIS), a nonprofit organisation established in October 2000. CIS Benchmarks encompass seven core technology categories and are developed through a unique, consensus-based process involving communities of cybersecurity professionals and subject matter experts worldwide.

1.3. "**CVSS**" or "**Common Vulnerability Scoring System**" is a method for capturing the primary characteristics of a vulnerability and assigning a numerical score that reflects its severity. The numerical score can then be translated into a qualitative representation (low, medium, high, and critical) to help organisations accurately assess and prioritise their vulnerability management needs. CVSS is a published standard used by organisations worldwide.

1.4. "**Device**" in the context of this Service Schedule means a single computer, tablet, mobile telephone, or other device (excluding Servers)

1.4.1. On which the licensee can install and use the Service Software, or;

1.4.2. The licensee can use Symantec's Infrastructure to enrol such devices for management by the Service. Processes.

1.5. **User and Device Licenses**:

1.5.1. "**User License**" means that the Customer may use the Service for up to the number of Users indicated in the Subscription.

1.5.2. "**Device License**" means that the Customer may use the Service for up to the number of Devices indicated in the Subscription.

1.5.3. The Customer may use a User license of the Service to protect multiple endpoint Devices of one User, OR use a Device license of the Service to protect a single Device of a User/ shared devices used by many users, provided that:

1.5.3.1. The customer must manage all such endpoint Devices for the Customer's internal business purposes and

1.5.3.2. The number of licensed endpoint Devices per User cannot exceed five. Customer may not use the Service to manage Customer's Users' personal Devices unless such personal Devices have been enrolled by Customer or the User to be managed by Customer for Customer's internal business purposes. Symantec Security Cloud Console allows the definition of security and access policies at the User level. Such policies apply to any Devices enrolled by a user, not to exceed 5 Devices per User.

1.6. "**User**" in the context of this Service Schedule means (i) a person authorised by Customer to use and benefit from the use of the Service, or (ii) who uses any portion of the Service. Each User provisioned in the subscription entitles the end user to deploy the Service on no more than five (5) Devices associated with that specific User.

1.7. **"Private applications"** refer to applications where the source code can't be downloaded from the internet without providing personal information or requiring a license key or license file. Private applications are not monitored for new versions; it's the customer's responsibility to provide SP with any resources for the initial packaging or any update afterwards, together with a procedure to install the application. SP can package these private applications as a separate chargeable engagement.

1.8. "**Public applications**" refer to publicly known and downloadable applications that do not require personal information, can be installed and executed silently, support disabling built-in auto-updates, and for which the license agreement doesn't prevent SP from making them available to SP's customers. These are applications where SP can access the sources on the vendor's website. They are monitored for new versions and are updated by SP. Public applications that do not support silent installations can only be requested as Private Applications.

1.9. "**Windows Autopilot"** refers to a collection of Microsoft Azure technologies used to set up and pre-configure new devices, thereby preparing them for productive use.

1.10. "**Workstation**" means a laptop or desktop device.

2. Service Overview

2.1. The Service provides access to the following:

2.1.1. Code Two Email branding for Exchange Online.

2.1.2. Monitoring and Compliance of security and compliance benchmarks:

Benchmark	Plan 1	Plan 2	Plan 3
CIS Microsoft 365 Foundation	Yes	Yes	Yes
CIS Microsoft Intune for Windows	-	Yes	Yes
CIS Microsoft Intune for Office	-	Yes	Yes
CIS Apple iOS and iPadOS for Intune	-	Yes	Yes
CIS Google Chrome		Yes	Yes
CIS Microsoft Edge		Yes	Yes
Android Enterprise	-	Yes	Yes

2.2. M365 Security and Compliance Plan 2 includes Endpoint Device Management, Application Management and Security Management using Microsoft Intune.

2.3. Bundle subscriptions include a **Device Rental Voucher and M365 Security and Compliance**. These Subscriptions are subject to the Service Schedule for Rental Services terms, incorporated by reference.

3. Standard Features

3.1. The following features of Plan 2 and Plan 3:

	Plan 2	Plan 3
Endpoint Security		
Antivirus Management	Yes	Yes
Disk Encryption	Yes	Yes
Firewall	Yes	Yes
Endpoint Privilege	Yes	Yes
Management	Yes	Yes
App Control for Business	Yes	Yes

Attack Surface Reduction	Yes	Yes
Account Protection	Yes	Yes
Conditional Access		
Microsoft Patch Management		
Silver SLA / Success Plan	CVSS > 8.9	CVSS > 8.9
Gold SLA / Success Plan	CVSS > 6.9	CVSS > 6.9
Platinum SLA / Success Plan	CVSS > 4.9	CVSS > 4.9
Third-Party Patch Management	Packaged Public Applications	Packaged Public Applications
One-Click Windows In-place Upgrade	Yes	Yes
Library of Pre-Packaged Applications	Yes	Yes
Private Package Management	Via Professional Services (charged separately)	Via Professional Services (charged separately)
Intune Management		
Configuration Profiles	Yes	Yes
Compliance Policies	Yes	Yes
Enrolment Policies	Yes	Yes
App Configuration Policies	Yes	Yes
Windows Autopilot deployment profiles	Yes	Yes
Enrolment Status Pages	Yes	Yes
Identity Management		
Conditional Access	Yes (Requires Professional Services)	Yes (Requires Professional Services)
Privileged Identity Mgmt	Yes (Requires Professional Services)	Yes (Requires Professional Services)
Endpoint Privilege Mgmt	Yes (Requires Professional Services)	Yes (Requires Professional Services)
Access Reviews		Yes (Requires Professional Services)
Entitlement Mgmt		Yes (Requires Professional Services)
Data Classification		
Sensitivity Labels		Yes (Requires Professional Services)
Cognni Autonomous Mapping		Yes (Requires Professional Services)
Data Loss Prevention		Yes (Requires Professional Services)

4. Application Package Management Pack

4.1. The Service includes deploying a catalogue of over 1000 pre-packaged Public Applications, which SP will automatically update.

4.2. If the Customer requires customising the pre-packaged applications or packaging of applications not pre-packaged by SP or a Private Application, the Customer will require a Professional Services Engagement, which is charged separately.

5. Additional Requirements for Plan 2 and Plan 3

5.1. Testing and Staging Account

5.2. The Customer is required to subscribe to at least one Plan 2 or Plan 3 subscription for testing and staging.

5.3. The Customer must also ensure that this account is assigned the appropriate Microsoft Licenses.

6. Customer Success Plan Entitlements

6.1. **Patch Management and Patch Policies**

6.1.1. These patch policies define (1) which patches need to be approved by SP, (2) if they require staging, (3) scheduling, and (4) how the agent should react in case of a reboot.

6.1.2. Depending on the Customer's Master Services SLA / Success Plan (Bronze, Silver, Gold or Platinum), Customers may have access to the following:

SLA / Success Plan	Bronze and Silver	Gold	Platinum
Automatically approve patches with **CVSS > 8.9**	Yes		
Manually approve patches with **CVSS > 6.9**	-	Yes	
Manually approve patches with **CVSS > 4.9**	-		Yes
Option to participate in staging groups	-		Yes

6.1.3. Platinum customers will also be entitled to allocate a subset of Customer devices to a staging group for initially staged patching. This approach ensures that approved patches can be tested on a limited number of devices and rolled back if necessary.

6.1.4. SP does not guarantee that patches will be free from defects or conflicts. The purpose of the staging group is to test vendor-approved patches in the field.

6.1.5. **Application patch management -**

6.1.5.1. SP will provide patch management for all pre-packaged Public Applications.

6.2. **Patch Management Exclusions**

6.2.1. Any Public Application that SP has not packaged;

6.2.2. All Private Applications

6.2.3. Non-Microsoft Operating Systems

6.2.4. Service Packs;

6.2.5. Language Packs

7. Pooled Support

7.1. Once the monitoring agents and security software have been successfully deployed, and SP has confirmed that the device meets its minimum supportability standards associated with the device:

7.1.1. SP will allocate **100 Pooled Support Units** for each **License** per month to be used for:

7.1.2. SP allocates all the **License** support units into a shared pool.

7.1.2.1. For example, if a Customer has ten devices, SP will allocate 1,000 (one thousand) Support Units per month. Assuming no Support Units have been used thus far in the month, the Customer will be entitled to use all 1,000 Support Units to address an issue on a single device.

7.1.3. If the Customer exceeds the Pooled Support allocation, (i) SP will not be required to provide support, and (ii) shall be entitled to charge for any assistance provided in excess of the allocated Pooled Support Units.

7.2. **Support Unit Exclusions**, each of which requires a separate Reserved Support Services or Application Package Management Subscription

7.2.1. Application Support;

7.2.2. Windows 10 Home Edition;

7.2.3. Support for devices without SP's remote monitoring agent pre-installed;

7.2.4. Support for connectivity problems;

7.2.5. Hardware-related issues, including but not limited to Hard Disk, Memory, Power Supply or the motherboard;

7.2.6. Migration services;

7.2.7. Telephonic support (other than a Company-Wide Workstation Deployment);

7.2.8. On-site support;

7.2.9. Service Pack or Language pack installation or troubleshooting;

7.2.10. Private Application package management.

9. Supported Devices

9.1. At the time of the release of this Service Schedule, the supported devices and operating systems are:

Device Type	Supported Operating Systems
Android	Android 8.0 and later (including Samsung KNOX Standard 3.0 and higher Android Enterprise
Apple	IOS 12 or later
macOS	Apple iOS 15.0 and later Apple iPadOS 15.0 and later macOS 11.0 and later
Windows Devices	Windows 10 Professional or Enterprise Windows 11 Professional

10. Security Responsibilities

10.1. The Service's end-to-end security is shared between SP and the Customer. SP will provide security for the Service's aspects over which it has exclusive physical, logical, and administrative control. The Customer is responsible for the aspects of the Service over which it has administrative-level access or control. The primary areas of responsibility between SP and the Customer are outlined below:

10.1.1. SP will use commercially reasonable efforts to provide the following:

10.1.1.1. **Information Security**: SP will protect the information systems used to deliver the Service over which it has sole administrative level control;

10.1.1.2. **Network Security**: SP will protect the networks containing its information systems to the extent that the Customer has control, permission, or access to modify the networks.

10.1.1.3. **Security Monitoring:** SP will monitor security events involving the underlying infrastructure servers, storage, networks, and information systems used in the Service's delivery, where it has exclusive administrative level control. This responsibility stops at any point where the Customer has some control, permission, or access to modify an aspect of the Service.

10.1.1.4. **Patching and Vulnerability Management**: SP will maintain the systems it uses to deliver the Service, including applying patches it deems critical for the target systems. SP will perform routine vulnerability scans to identify critical risk areas for its systems, enabling the delivery of the Service. Critical vulnerabilities will be addressed promptly.

10.1.1.5. **Security Monitoring**: The SP is responsible for detecting and classifying all security events that surface through the Service vulnerability scanning tools.

10.1.2. The Customer is responsible for addressing the following:

10.1.2.1. **Information Security:** The Customer is responsible for ensuring the adequate protection of the information systems, data, content, or applications it deploys or accesses through the Service. This responsibility includes, but is not limited to, patching at

all levels, implementing security fixes, encrypting data, establishing access controls, and assigning roles and permissions to internal, external, and third-party users.

10.1.2.2. **Network Security:** The Customer is responsible for the security of the networks over which it has administrative-level control. This responsibility includes, but is not limited to, maintaining effective firewall rules, exposing only necessary communication ports for business purposes, and restricting promiscuous access.

10.1.2.3. **Security Monitoring**: The Customer is responsible for remediation of all security events isolated from their Service account, associated with operating systems, applications, data, or content surfaced through vulnerability scanning tools or required for a compliance or certification program in which the Customer must participate. If the customer requires SP's assistance with remediation, (i) SP will not be required to provide support, and (ii) shall be entitled to charge for any assistance provided.

11. Metering and Billing

11.1. SP uses an Enterprise Application, the Customer's Microsoft 365 tenant, to count:

11.1.1. The number of Microsoft Licenses with an Exchange Mailbox,

11.1.2. the number of Intune Devices, and

11.1.3. the number of Microsoft Licenses with an Intune entitlement.

11.1.4. SP will increase the quantity billed whenever an increase in licences is detected.

11.1.5. SP will decrease the number of licences on the subscription anniversary to match the Customers' license counts.

11.2. **User-Based Licensing – Plan 1:**

11.2.1. Every assigned Microsoft license with a Microsoft Exchange Online entitlement assigned to a user will be counted as billable.

11.2.2. The list (which is subject to change without notice) of Microsoft licences that are in scope and have a Microsoft Exchange Online entitlement is currently:

11.2.2.1. Microsoft 365 Business Basic

11.2.2.2. Microsoft 365 Business Standard

11.2.2.3. Office 365 E1

11.2.2.4. Office 365 E5

11.2.2.5. Exchange Online Plan 1

11.2.2.6. Exchange Online Plan 2

11.3. **User-Based Licensing – Plan 2 and Plan 3:**

11.3.1. Every assigned Microsoft license with a Microsoft Intune entitlement assigned to a user will be counted as billable.

11.3.2. Customers must be either on Plan 2 or Plan 3. A combination of Plan 2 and Plan 3 is not permitted.

11.3.3. The list (which is subject to change without notice) of Microsoft licences that are in scope and have a Microsoft Intune entitlement is currently:

11.3.3.1. Microsoft 365 Business Premium

11.3.3.2. Microsoft 365 F1

11.3.3.3. Microsoft 365 F3

11.3.3.4. Microsoft 365 E3

11.3.3.5. Microsoft 365 ES Enterprise Mobility + Security E3

11.3.3.6. Enterprise Mobility + Security E5

11.3.3.7. Microsoft 365 Government G3

11.3.3.8. Microsoft 365 Government G5

11.3.3.9. Intune for Education

11.3.3.10. Microsoft 365 Education A3

11.3.3.11. Microsoft 365 Education A5

11.3.3.12. Microsoft Intune Device

11.3.4. If a user has multiple computers, we will update the applications on all their devices if the application is assigned to that user and the devices are enrolled in Intune.

12. Professional Services Engagements

12.1. The deployment and configuration of the service require professional service engagements, which are charged separately. Professional Service Engagement is required for:

12.1.1. **Hybrid Identity:**

12.1.1.1. Deploy Entra Connect and Entra Connect Health and synchronise user identities between the on-premises Active Directory Domain Services (AD DS) and Entra.

12.1.2. **Azure AD Domain Services (also known as Entra Domain Services):**

12.1.2.1. Configure Azure AD Domain, DNS, Single Management Server, and Security Groups for VPN Access.

12.1.3. **Plans 1, 2 and 3:**

12.1.3.1. Exchange Online, Teams, Groups and OneDrive and 365 Tenant Best Practices: Unified Log Search, Modern Authentication, Defender for Office 365 Policies, Disable Legacy Authentication, Disable Auto Forwarding, Configure Deleted Item Retention, Configure SPF, DMARC and DKIM (Managed domains only), Configure Mailbox Audit Log, Disable Consumer Storage Locations, Configure Break Glass Accounts. Configure Email Signature, Journal Report Decryption, Temporary Access Passwords, Admin Approved Authentication Methods, and Passwordless Sign-in. Enforce security and compliance policies for permissions and access controls, including those for external users. Automatically detect, notify, and revert configuration drift and security issues.

12.1.4. **Plan 2:**

12.1.4.1. Endpoint Management: Enrolment of Pilot Devices, Project Management, Policy Review, App Catalogue Setup, Azure Active Directory Tenant Branding, Intune Deployment of Autopilot, Application Management, Endpoint Security, Intune Policies and Profiles configuration of the following Benchmarks: CIS Microsoft Intune for Windows, CIS Microsoft Intune for Office, CIS Apple iOS and iPadOS for Intune, CIS Google Chrome, CIS Microsoft Edge, and Android Enterprise.

12.1.4.2. Conditional Access and Privileged Identity Management: Conditional Access provides automated access control decisions for users to access cloud apps based on specific conditions. Privileged Identity Management offers time-based and approval-based role activation to mitigate the risks associated with excessive, unnecessary, or misused access permissions on critical resources.

12.1.5. **Plan 3:**

12.1.5.1. Access Reviews: Microsoft Entra ID Access Reviews are a critical component of Microsoft Entra's identity governance capabilities. They enable organisations to manage group memberships, application access, and role assignments efficiently and effectively. Regular reviews of user access ensure that only authorised individuals maintain access rights, thereby enhancing security and compliance.

12.1.5.2. Entitlement Management: Microsoft Entra ID Entitlement Management is an identity governance feature that automates the lifecycle management of identity and access. It streamlines access request workflows, assignments, reviews, and expirations for groups, applications, and SharePoint Online sites. Designed for scale, it simplifies managing access rights, especially in dynamic environments and when collaborating with external organisations. It addresses challenges like unknown access needs and prolonged access retention. It offers solutions such as multi-stage approval processes, time-limited assignments, and recurring access reviews to ensure appropriate access control within and across organisational boundaries.

12.1.5.3. Sensitivity Labels: Microsoft Sensitivity Labels are a feature within Microsoft Purview Information Protection that allows organisations to classify and protect their data. These labels can be applied to documents, emails, and other content to enforce

security measures, such as encryption and content markings, including watermarks, headers, and footers. Sensitivity labels ensure that data is handled according to its level of confidentiality, even when shared outside the organisation. They support compliance by keeping content secure across various platforms, including third-party apps and services. This protection travels with the content, maintaining security wherever the data goes.

12.1.5.4. Data Leakage Prevention: Microsoft Data Loss Prevention (DLP) is part of Microsoft Purview, designed to protect sensitive information across various platforms and devices. It helps organisations prevent unauthorised sharing, access, and transmission of sensitive data. DLP policies can be applied across Microsoft 365 services, Windows 10 and Windows 11, macOS endpoints, and non-Microsoft cloud applications. It utilises deep content analysis, machine learning, and other advanced methods to identify and protect sensitive data. Microsoft DLP is suitable for those within the Azure ecosystem, offering centralised policy controls for a comprehensive data security solution.

13. Use of SP's Intellectual Property

13.1. **Non-transferable perpetual right of use of this intellectual property beyond the termination of the Subscription**

13.1.1. The configuration elements listed below form part of the SP's sole intellectual property:

13.1.1.1. Conditional Access Policies deployed by SP

13.1.1.2. Defender for Office 365 Policies deployed by SP

13.1.1.3. Endpoint Security Anti-Virus Polices deployed by SP

13.1.1.4. Disk Encryption Policies deployed by SP

13.1.1.5. Firewall Policies deployed by SP

13.1.1.6. Endpoint Detection and Response Policies deployed by SP

13.1.1.7. Attack Surface Reduction policies deployed by SP

13.1.1.8. Account Policies deployed by SP

13.1.2. Provided the Customer has not and does not breach this Agreement, SP grants the Customer a non-transferable, perpetual right to use this intellectual property within their existing Microsoft Tenant beyond the termination of the Subscription.

13.1.3. The Customer treats these elements as confidential and shall not export, copy, migrate, clone, duplicate or otherwise share these elements with any third party.

13.2. **Non-transferable non-perpetual right of use of this intellectual property for the duration of the Subscription**

13.2.1. The configuration elements listed below form part of the SP's sole intellectual property:

13.2.1.1. Logic Apps deployed by SP

13.2.1.2. Intune Policy Sets deployed by SP

13.2.1.3. Intune Configuration Profiles deployed by SP

13.2.1.4. Intune Policies not listed in 13.1 above.

13.2.1.5. Packaged Public Applications deployed by SP

13.2.1.6. Packaged Private Applications deployed by SP

13.2.1.7. Scripts deployed by SP

13.2.2. Custom Sensitive Information Types (SITs) in Microsoft Purview.

13.2.3. Provided the Customer has not and does not breach this Agreement, SP grants the Customer a non-transferable, non-perpetual right to use this intellectual property within their existing Microsoft Tenant for the duration of the Subscription.

13.2.4. The Customer treats these elements as confidential and shall not export, copy, migrate, clone, duplicate or otherwise share these elements with any third party.

13.2.5. SP shall be entitled to access the Customer's environment and remove these configuration elements (i) upon termination of the Subscription or (2) if the Customer breaches this agreement.

14. M365 Security and Compliance + Device Rental Vouchers

14.1. Bundle subscriptions include a **Device Rental Voucher and M365 Security and Compliance**.

14.2. These Subscriptions are subject to the Service Schedule for Rental Services terms, incorporated by reference.