Exhibit A to Additional Terms for Ricoh Work Anywhere Services
Ricoh Work Anywhere Service Brief

Ricoh Work Anywhere Service Bundles:

The Ricoh Work Anywhere Services ("RWA") are delivered as a bundled offering. Each bundle, as described below, represents various levels of Ricoh involvement and engagement with the customer, as well as supported features and capabilities.

RWA Bundle Differentiation	Ricoh Work Anywhere	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe +
Customer Success & Service Reviews	Quarterly	Quarterly	Monthly
Business Review with Customer Executive	Annual	Annual	Quarterly
Ricoh Technology Health Score Reports	Annual	Annual	Quarterly
Microsoft Secure Score Reports	Semiannual	Semiannual	Quarterly
Cloud & Digital Work Strategy & Road mapping Engagements	Semiannual	Semiannual	Quarterly
Microsoft Vulnerability* Reports			Quarterly
Microsoft Data Loss Prevention (DLP)* for emails and files			Included
Microsoft Intune Company Portal*			Included

*Refer to Microsoft for definitions above Microsoft products and services

RWA Enhanced Security Features by bundle:

Each RWA bundle also includes one, or more, enhanced security features as described in the table below.

RWA Bundle - Security Differentiation	Ricoh Work Anywhere	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe +
Managed Adoption Services: Basic features	Included	Included	Included
Managed Adoption Services: Simulated Phishing Campaigns		Included	Included
Managed Adoption Services: Custom Content Publishing			Included
Managed Security Services		Included	Included
Managed Web Filtering: core features see service description		Included	Included
Managed Web Filtering: Configure and maintain specific content filtering policy			Included

Ricoh Work Anywhere – Add-On Services

On top of the RWA bundle chosen by the Customer, the Customer may also elect to include one or more of the below "Add-On Services" in addition to the RWA bundle.

Mobile Device Management	Mobile Device Management – Create policies for mobile devices that control End User identity sign in, installed apps, and data accessed

Desktop Anywhere	Access your work desktop from any device with an internet connection. End Users can seamlessly switch between devices accessing their Desktop Anywhere as it was on the initial device and with the same performance. This enables businesses to spend less on End User devices as Desktop Anywhere only requires a reliable internet connection and a supported device to stream to. Desktop Anywhere may be rapidly deployed, restored & retired, enabling business to quickly scale their environment. Also includes Microsoft Intune Security Baseline configuration and anti-endpoint protection on virtual desktop.

Desktop Anywhere +	Includes Desktop Anywhere as described above. Managed Security Service installed in the Desktop Anywhere environment. Managed Web Filtering installed in the Desktop Anywhere environment.

Ricoh Work Anywhere Core Service:

The below service components are included in all RWA bundles.

Customer Success & Advisory Services

Customer Success Manager	Service Review and reporting with Customer IT Manager:
	- Ricoh Technology Health Score:
	- M365 Productivity Score
	- M365 Secure Score
	- M365 Compliance Score
	- M365 Service Utilization Analytics
Technology Advisory Consultant	Cloud & Digital Work Strategy & Road-Mapping Engagements:
	- Identify IT business goals
	- IT Services roadmap development & progress tracking

Account Management and Employee Helpdesk

Employee Helpdesk & Support	Ricoh Portal, Telephone, Email, Chat
	7am-7pm (M-F) remote
Microsoft Windows OS Quality Updates	Monthly update that includes bug fixes, feature improvements, and security issue resolutions.
Microsoft Windows OS Feature Updates	Annual update that contains new features.

Security Capabilities

Azure Active Directory*	Multi Factor Authentication & Conditional Access: identity authentication based on region/time
	End User, Groups & Admin Role Account Management
Intune*	Windows Endpoint Security Baseline Configuration
	Windows Mobile Application Management (MAM)
Defender for Office 365*	Email filtering: anti phishing, malware, spam
	OneDrive/SharePoint/Teams link and attachment protection
Endpoint Anti-Malware Protection*	Static Malware Detection and Response
Bitlocker*	Windows Endpoint Encryption
Windows Autopilot*	Endpoint lifecycle management: Cloud endpoint deploy, restore, retire/re-assign
Microsoft 365 Backup & Restore*	Emergency data back-up
Managed Adoption Services	Basic features: see serv desc.

* These capabilities are available under the Microsoft license. Through RWA, Ricoh manages and configures above Security Capabilities.

”Managed Adoption Service”:

Ricoh Managed Adoption Service management is provided by Ricoh as a remote services model. Details of this offering are outlined in the below “Roles and Responsibilities” section.

Service Components	Ricoh Work Anywhere	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe +
Office/Microsoft 365 Training and Adoption	Included	Included	Included
Security Awareness Training	Included	Included	Included
Simulated Phishing Campaigns		Included	Included
Custom Content Publishing			Included

Managed Adoption Service Roles and Responsibilities

Description	Ricoh Work Anywhere	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe +
Content Management			
Maintain an inventory of Office/Microsoft 365 and security awareness training content.	Ricoh	Ricoh	Ricoh
Develop Office/Microsoft 365 learning paths based on services in use, employee proficiency level, and organizational goals.	Ricoh	Ricoh	Ricoh
Create and maintain customer specific Office/Microsoft 365 training schedule.	Ricoh	Ricoh	Ricoh
Develop security awareness learning paths based on relevant threat vectors and organizational goals.	Ricoh	Ricoh	Ricoh
Create and maintain customer specific security awareness training schedule.	Ricoh	Ricoh	Ricoh
Host a monthly service review, campaign analysis and roadmap development meeting.	Ricoh	Ricoh	Ricoh
Simulated Phishing Campaigns			
Maintain an inventory of simulated phishing campaigns.		Ricoh	Ricoh
Conduct quarterly simulated phishing campaign to test employee security awareness.		Ricoh	Ricoh
Assign remedial training for employees who fail to meet organizational security standards.		Ricoh	Ricoh
Provide simulated phishing campaign analysis.		Ricoh	Ricoh
Custom Content Publishing			
Create custom employee training content. Examples of this content may include the following. • Videos • PDFs • Office documents (Excel, Word, PowerPoint) • Graded and non-graded assessments			Customer
Up two (2) hours of Ricoh Service Adoption Specialist time per month to complete the following, upon request. • Manage existing custom content/learning paths • Publish new custom content • Create required learning path(s) • Assign custom learning path(s) to employees			Ricoh

• Provide training campaign analysis			
Administration			
Review and approve content updates for existing learning paths.	Ricoh	Ricoh	Ricoh
Manage interoperability of training and adoption platform and Office/Microsoft 365 services. Examples of these services may include the following. • Azure Active Directory • Microsoft Graph • Defender for Office 365 or Exchange Online Protection • Exchange Online • Teams	Ricoh	Ricoh	Ricoh
Escalate support incidents to vendor support at Ricoh's discretion	Ricoh	Ricoh	Ricoh

”Managed Web Filtering Services”:

Ricoh Managed Web Filtering provided by Ricoh as a remote services model. Details of this offering are outlined in the below “Roles and Responsibilities” section.

Service Components	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe +
DNS server based malicious domain filtering - DNS server based filtering utilizes existing DNS servers, be it a server operating system based DNS server such as a domain controller or network perimeter device acting as a DNS server such as a firewall to provide malicious domain filtering. All DNS queries which originate from within the business networks for external domains are routed through these existing DNS servers which filter the results through the Ricoh Managed Web Filtering service to block and thus prevent access to malicious domains	Included	Included
Agent based malicious domain filtering – Agent based filtering utilizes a lightweight agent which is installed on End User endpoint devices, be it a laptop, desktop, or server. This agent enables the same malicious domain filtering functionality as the DNS server based filtering but expands upon it by removing the requirement of being on business network for protection. Thus, enabling endpoint protection from malicious domains anywhere, be it a wired or wireless network located at home, a hotel, a coffee shop, etc	Included	Included
DNS server and agent based content filtering - – Expanding upon the DNS server and agent based malicious domain filtering the Ricoh Managed Web Filtering service offers content based filtering. When leveraging this functionality, the above mentioned filtering mechanisms are expanded upon not only filtering malicious domains but also specified content types thus preventing access to content restricted domains		Included

Each tier includes the following Ricoh managed services.

- Ricoh Work Anywhere Safe – Web Filtering Core features:
    - Manage Ricoh developed malicious domain filtering policies
    - Manage Ricoh developed domain specific allow/deny lists
    - Provide monthly malicious domain filtering report
    - Configure managed DNS servers and/or perimeter devices for forwarding of DNS queries
    - ALL features of the Basic service tier plus the following
    - Configure and maintain customer specific domain allow/deny lists
    - Deploy lightweight agent to managed endpoints

- Ricoh Work Anywhere Safe +
    - All above features
    - Configure and maintain customer specific content filtering policy

Managed Web Filtering Roles and Responsibilities

Description	Ricoh Work Anywhere Safe		Ricoh Work Anywhere Safe +	
	Ricoh	Customer	Ricoh	Customer
Malicious Domain Filtering				
Manage Ricoh developed malicious domain filtering policies.	X		X	
Manage Ricoh developed domain specific allow/deny lists.	X		X	
Develop and maintain custom domain specific allow/deny lists.		X		X
Configure and maintain domain specific allow/deny lists based on customer provided requirements	X		X	
Leverage Cisco Umbrella agent for malicious domain filtering on and off the corporate network.	X		X	
Provide a monthly malicious domain filtering report.	X		X	
Content Filtering				
Develop and maintain content filtering policy based on available categories.				X
Configure and maintain content filtering policy based on customer provided policy requirements.			X	
Leverage Umbrella agent for content filtering on and off the corporate network.			X	
Provide a monthly content filtering report.			X	
Administration				
Deploy Umbrella agent to managed endpoints (servers and workstations).	X		X	
Configure managed DNS servers for forwarding of DNS queries.	X		X	
Configure managed perimeter devices acting as DNS servers for forwarding (if supported).	X		X	
Escalate support incidents to vendor support at Ricoh's discretion.	X		X	

“Managed Security Services”:

The Managed Security Service solution is comprised of five underlying layers of protection:

- Prevent – Static AI in the SentinelOne Singularity agent provides on and offline pre-execution protection for End User endpoints from known threats.

- Detect – Behavioral AI in the Singularity agent provides on and offline protection from unseen, unknown, or novel malware for End User endpoints. Storyline tracks the actions of an attack from beginning to end across endpoints.

- Respond – The Singularity agent automatically quarantines malicious files, kills bad processes, and stops bad services. When the endpoint is connected to the internet, the Singularity agent alerts the 24x7 Vigilance SOC of the event for investigation and Ricoh Security Team engagement.

- Recovery – As part of a post incident response, Storyline enables a step-by-step review of an event as well as provides one-click rollback on Singularity protected endpoints running a supported Windows operating system versions.

- Hunt – “Active-EDR” enables deep visibility into 90 days of historical data across an organization for enhanced threat hunting to uncover advanced adversaries.

Combined, provide the advanced multi layered security required to protect End User endpoints from modern day threats.

Dark Web Monitoring

The Kaseya Dark Web ID solution regularly scans the Dark Web including hidden chat rooms, unindexed sites, private sites, peer-to-peer networks, Internet Relay Chat (IRC) channels, social media platforms, and black-market sites for credentials related to your organization. Dark Web ID leverages your company’s public domain(s) to search for any reference to identities including items such as End Usernames, passwords, and Personally Identifiable Information (PII) including first and last name, address, phone number, social security number, banking information, etc. Upon detection, named Points of Contact (POCs) are notified and can view the incident details so that they may engage the impacted End Users to facilitate the necessary password changes.

Managed Security Services Roles and Responsibilities

Management Description	Responsibility	
	Ricoh	Customer
Monitoring, Response, and Updates		
24/7 monitoring and response by the SOC for SentinelOne Singularity detected events which may include the following. · Quarantining malicious files · Killing bad processes · Stopping bad services · Executing complete device quarantine/isolation	X	

· Initiating Storyline powered one click rollback on supported managed endpoints to restore device configuration, applications, End User settings, and/or files to a state before the attack began v Responses are limited to the extend the Singularity agent can do so		
Escalate SentinelOne detected events to the Ricoh Security Team for further review and engagement at the discretion of the SOC	X	
Ricoh Security Team support for incidents escalated by the SOC · Incident and response review with Vigilance SOC · Incident review leveraging Storyline and Active EDR · Point of contact (POC) engagement for incident review · Provide advisory services in the event of a security incident which may include referral to 3rd party cybersecurity vendor(s)	X	
Initiate full IR plan development and execution · X^1 – Customer may engage cybersecurity vendor of their choosing · X^2 – Customer may elect to engage Ricoh and Ricoh partnered cybersecurity vendors for a time and materials engagement to aid in the development and execution of an incident specific IR plan. The scope of the engagement will be tailored to the customer's specific needs and be presented in an optional SOW.	X^2	X^1
Apply SentinelOne Singularity agent updates at Ricoh's discretion	X	
Escalate support incidents to SentinelOne and/or Kaseya at Ricoh's discretion	X	
Administration		
Conduct ad-hoc on-demand environment scans on systems running the SentinelOne Singularity agent	X	
Review false positives and update SentinelOne exclusion list as necessary	X	
Collaboratively review and attempt remediation for performance related issues on systems running the SentinelOne Singularity agent	X	X
Notify Ricoh of additional public domains requiring or existing public domains no longer requiring Dark Web ID monitoring		X
Update Dark Web ID to reflect active company public domains requiring monitoring. Up to two public domains are included additional public domains may be added as a separate billable line item.	X	
Confirm SentinelOne Singularity agent installation on newly provisioned or reprovisioned managed endpoints. · X^1 – Customer provisioned managed endpoints · X^2 – Ricoh provisioned managed endpoints	X^2	X^1
Provide End User notification of compromised credentials and/or Personally Identifiable Information (PII) reported by Dark Web ID and oversee remediation efforts		X
Recovery		
Initiate backup based restore of impacted endpoints when applicable · X^1 – Customer will restore impacted files and folders	X^2	X^1

· X^2 – Unless covered under managed backups services, customer may elect to engage Ricoh for a time and materials engagement to aid in the restore. The scope of the engagement will be tailored to the customer's specific needs and be presented in an optional SOW.		
Initiate rebuild/reimage of impacted endpoint(s) · X^1 – Customer will conduct the rebuild/reimage of impacted endpoint(s). · X^2 – Customer may elect to engage Ricoh for a time and materials engagement to aid in the rebuild/reimage. The scope of the engagement will be tailored to the customer's specific needs and be presented in an optional SOW.	X^2	X^1

Ricoh Work Anywhere Add-on Service "Desktop Anywhere":

Virtual Desktop in the Cloud

- Enhanced security posture – Desktop Anywhere is inherently more secure than physical computers as all Desktop Anywhere compute, storage, and memory resources are in the same secure cloud as Microsoft Azure and Microsoft 365. Additionally, Desktop Anywhere expands on the security measures configured in Ricoh's Managed Digital Work Services powered by Microsoft 365. This includes access to Desktop Anywhere and the applications and resources they have access to being secured with multi-factor authentication, conditional access, and other security policies to prevent data exfiltration.

- Stream to any device – Desktop Anywhere are Windows 10 or 11 PCs that are not directly running on an employee's endpoint device be it a laptop or desktop. Thus Desktop Anywhere is accessible from most modern devices running Windows 10 or 11, Mac OS, iOS, or Android. This diversity enables employees to have the same full featured Windows 10 or 11 experience on any device be it a company issued or personal computer, tablet, or phone. Employees are even able to seamlessly switch between devices accessing their Desktop Anywhere as it was on the initial device and with the same performance.

- Minimize capital expenditures – Desktop Anywhere enables businesses to spend less on employee devices as Desktop Anywhere only requires a reliable internet connection and a supported device to stream to. Thus, businesses may procure entry-level/light-duty computers and/or allow leveraging personal devices while still providing the performance employees need to work effectively.

- Scale on-demand – Desktop Anywhere may be rapidly provisioned and/or resized enabling business to quickly scale their environment with no lead-time on hardware, impact related to supply chain disruptions, or depots for configuration.

- Seamless configuration – Desktop Anywhere is configured and managed with the same policies and tools used for physical computers. This enables businesses to configure physical Desktop Anywhere consistently in the same manner allowing simplified configuration management and a seamless End User experience across devices.

- Resilience and recoverability – Desktop Anywhere is built on Microsoft Azures robust and highly resilient infrastructure virtually eliminating infrastructure related downtime. Additionally, Desktop Anywhere allows for up to 10 days of recovery points enabling a quick restore of a Desktop Anywhere to a previous state in the event of an operating system or application related issue.

Desktop Anywhere Configuration and Support Service Tiers

Tier	Use Case	CPU Cores	RAM (GB)	Storage (GB)
Basic	Ideal for occasional access, frontline workers*, interns, or contractors	2	4	128
Standard	Ideal for most employees using traditional business applications	2	8	128
Advanced	Ideal for employees using applications which require higher performance	4	16	128

** Frontline workers, who often work on tablets or phones and work either directly with customers or the general public. They provide services, support, and sell products, or are employees directly involved in the manufacturing*

and distribution of products and services. For example: retail associates, healthcare clinicians and nursing staff, factory workers, and so on.

Desktop Anywhere Roles and Responsibilities

Desktop Anywhere	
Description	Responsibility
License management • Procurement • Assignment • Reassignment • Removal	Ricoh
Infrastructure management • Configuration profiles • Configuration groups • End User settings • Azure network connections	Ricoh
Lifecycle management • Provision • Reprovision • Restore • Resize • Remove	Ricoh
Deployment and configuration • Desktop Anywhere deployment • Intune managed application(s) installation • Anti-malware protection installation • Ricoh support tools installation • Known folder redirection configuration • Security baseline configuration • Attack surface reduction configuration • Ricoh in depth security configuration	Ricoh
Applicable operating system updates • Windows quality updates • Windows feature updates	Ricoh
Support Services • Point of contact (POC) support • Employee support • Support contact options • Support incident escalation	Ricoh

RWA Bundle + Add-On Services Compatibility

		Add-on Services		
		Mobile Device Management	Desktop Anywhere	Desktop Anywhere +
Ricoh Work Anywhere	Scenario 1	✓		
	Scenario 2		✓	
	Scenario 3	✓	✓	
Ricoh Work Anywhere Safe	Scenario 4	✓		
	Scenario 5			✓
	Scenario 6	✓		✓
Ricoh Work Anywhere Safe +	Scenario 7	✓		
	Scenario 8			✓
	Scenario 9	✓		✓

Ricoh Work Anywhere Fee Structure:

Ricoh Work Anywhere	Monthly Recuring Management Fee
Implementation Fee	Monthly Professional Services - first 12 months only

Ricoh Work Anywhere Enrollment Conditions

Minimum enrollment requirements:

- A minimum of 50 End Users are enrolled in Ricoh Work Anywhere Subscriptions
- Matching End User enrollment in corresponding Ricoh-supported Microsoft 365 Subscriptions
- All workstations are joined to either Azure Active Directory or Hybrid Azure Active Directory

A Microsoft 365 license is required for every Ricoh Work Anywhere End User. Ricoh recommends that the customer select their Microsoft 365 license in accordance with the size of their End User base. The below table differentiates which Microsoft 365 license licenses Ricoh offers in combination with Ricoh Work Anywhere.

License Plan	Workforce Size
Microsoft 365 Business Premium	SMBs under 300 office workers.
Microsoft 365 E3 + Defender for Office 365 Plan 1	Enterprises with 300+ office workers.
Microsoft 365 F3 + Defender for Office 365 Plan 1	SMB or Enterprise field workers.

Microsoft Subscriptions & Licensing:

Ricoh requires the requisite Microsoft subscriptions be procured via Ricoh's partnership with Microsoft's Cloud Service Provider (CSP) program. All Microsoft subscriptions are provided by Ricoh as annual subscriptions, billed monthly to the customer. When possible, Ricoh will endeavor to make Microsoft subscription expiration dates coterminous. The customer is responsible for the full-term value of any Microsoft subscription. All Microsoft subscriptions will be set to auto-renew when term expiration is reached.

Ricoh Bring Your Own Licensing (BYOL) Program:

Alternatively, Ricoh will accept Microsoft subscriptions procured by means other than Ricoh's CSP program under these conditions:

1. The customer is transitioning from another Managed Services Provider (legacy MSP) to Ricoh Managed IT Services:
    a. Existing Microsoft subscriptions attributed to the legacy MSP that cannot be transferred to Ricoh:
        i. Ricoh is designated as the Customer Partner of Record (CPOR) with Microsoft.
        ii. Legacy MSP subscriptions must be set to "do not auto-renew" in Microsoft's management portal.
        iii. Upon service implementation and onboarding with Ricoh, new requisite subscriptions must be created under Ricoh's CSP program with a minimum quantity of (1) license per subscription.
        iv. Ricoh will apply an administrative fee per subscription/license provided by the legacy MSP.
        v. All further Microsoft subscriptions and licenses are purchased under Ricoh's CSP program.
        vi. As legacy MSP subscriptions expire, matching subscriptions and licenses are procured under Ricoh's CSP program and applied to affected End Users.
        vii. Administration fees associated with Legacy MSP subscriptions & licenses will be dropped as legacy MSP subscriptions expire.
2. The customer is obliged to purchase requisite subscriptions from other providers due to parent company or other mandates beyond the customer's control:
    a. Upon service implementation and onboarding with Ricoh, new requisite subscriptions must be created under Ricoh's CSP program with a minimum quantity of (1) license per subscription.
    b. Ricoh will apply an administrative fee per subscription/license provided by the other provider.

For clarity, and notwithstanding anything to the contrary, Microsoft subscriptions are not provided as part of the Ricoh Work Anywhere Services and must be purchased separately under a separate contract; and, for such subscriptions all Microsoft licensing terms and conditions apply.

Technical Prerequisites:

Deployment and Management of RWA Safe and RWA Safe+ Bundles require the following:

- The customer purchase Ricoh Workstation Management and Server Management
- Device operating systems can support Cisco Umbrella
- Device operating systems can support SentinelOne

Deployment and Management of Desktop Anywhere Add-On requires the following:

- A minimum of 5 End Users are enrolled in Ricoh Desktop Anywhere Subscriptions
- Matching End User enrollment in corresponding Ricoh Work Anywhere Subscriptions
- Matching End User enrollment in corresponding Ricoh-supported Microsoft 365 Subscriptions