Exhibit B: Service Description for Ricoh Work Anywhere

Table of Contents

Unauthorized Use Prohibited

This document and its contents are intended for client use and reference only. Unauthorized use, reproduction, or distribution of this document to parties other than Ricoh or a Ricoh client enrolled in the services described in this document are prohibited.

Service Description for Ricoh Work Anywhere Essentials

Overview

What is Ricoh Work Anywhere Essentials?

Ricoh Work Anywhere Essentials is the foundational component service of all Ricoh Work Anywhere bundles, and is designed to:

- Provide a Ricoh designed & configured hybrid work core solution for users.
- Include user support, administration, and solution management services.

Ricoh Work Anywhere Essentials Service Features

Ricoh Work Anywhere Essentials integrates solutions and features with valuable Ricoh-provided services delivered by hybrid work experts:

- Standardized Best Practice service & solution configuration developed by Ricoh.
- Zero-Trust based security baseline developed by Ricoh that conforms to CIS standards for identity, device, application and data protections.
- Professional implementation of Ricoh Work Anywhere Essentials and onboarding of users into the service with minimal (if any) disruption.
- End user helpdesk, support, and administrative services provided by Ricoh cloud and hybrid work specialists.
- Client Success Management and Technology Advisory services that are devoted to achieving successful business outcomes and value realization for our clients.
- Ongoing lifecycle management of the service and solutions that keeps Ricoh Work Anywhere modern, current and relevant in a rapidly changing technology ecosphere.

Ricoh Work Anywhere Essentials Service Tiers

There are three tiers of service for Ricoh Work Anywhere Essentials:

Basic	Advanced	Premium
Included in RWA Small Business Bundle Easy point-of-adoption choice for customers who seek to control cost by adopting a shared responsibility model for Microsoft 365 administration and support workloads. This tier of service is a shared responsibility model between Ricoh and the customer. The customer is responsible for general user administration and first-level support for user incidents and problems. The customer's designated points of contact with Ricoh (POCs) can escalate larger issues to Ricoh Support. Ricoh is responsible for the configuration and management of the Microsoft 365 solution. This level of service includes limited availability to Ricoh add-on services and service enhancements.	**Included in RWA & RWA Safe Bundles** Designed for companies that seek a provider-operated solution and services to reduce in-house IT workloads and burdens. This tier of service includes all of the value of Basic, plus the following: • Higher level of Customer Success and Technology Advisory engagement. • Ricoh is responsible for end user support. End users and Client Representatives may report support incidents to Ricoh directly for incident response, escalation, and resolution. • Ricoh is responsible for user and solution administration and management. • More Microsoft 365 supported features. • More availability to Ricoh add-on services and service enhancements.	**Included in RWA Safe Plus Bundle** The service choice for companies seeking Ricoh's maximum level of service value and capabilities. This tier of service includes all the value of Advanced, plus: • Maximum level of Customer Success and Technology Advisory engagement. • Maximum level of Microsoft 365 feature support. • Availability to all available Ricoh Work Anywhere add-on services and service enhancements.

Microsoft Subscription Requirements

Ricoh Work Anywhere requires specific Microsoft subscriptions and licensing. All users enrolled in the service need to be assigned one of the Microsoft 365 Subscription choices shown below:

Microsoft 365 Subscription Choices		Workforce Type
1.	**Microsoft 365 Business Premium**	Companies under 300 Information (office) workers that prioritize office information systems and workflows, teamwork collaboration, and communications with co-workers and clients.
2.	**Microsoft 365 E3 + Defender for Office 365 Plan 1**	Companies with 300+ Information (office) workers that prioritize office information systems and workflows, teamwork collaboration, and communications with co-workers and clients.
3.	**Microsoft 365 F3 + Defender for Office 365 Plan 1**	Companies that have a Frontline (field / facility) workforce that prioritizes mobility, access to applications and real-time communications. This plan differs from choices 1 & 2 in the following manner: • Reduced Mailbox, One Drive, Teams, and SharePoint capacities • No email Archiving & Litigation Hold • No public folder mailboxes • No desktop Office 365 applications • No Data Loss Prevention for emails & files Components may change. For current subscription comparisons, refer to Microsoft official documentation.
Shared (Resource) Mailboxes		Resource Mailboxes are not assigned to a user account. These are general-use mailboxes with access by multiple employees or groups within a client company. In addition to the above user licensing choices, each Resource Mailbox requires Defender for Microsoft 365 licensing.

Different segments of the client's workforce can be assigned different Subscription choices to suit the workforce needs. For example, a company may have an office workforce and a field-based workforce. The Office workforce users can be assigned choice #1 or #2 above, and the field-based workforce can be assigned choice #3 (which is a lower cost but less capability).

Microsoft terms and conditions apply.

Bring Your Own Licensing Program

Microsoft subscriptions are purchased separately and procured for the client through Ricoh's partnership program with Microsoft. For the purposes of service delivery and management, Ricoh will at minimum create the required Microsoft subscriptions with one license per subscription under Ricoh's partner program with Microsoft.

The client will purchase all new Ricoh Work Anywhere Microsoft licensing through the Ricoh-provided subscriptions.

If the client already possesses the required Ricoh Work Anywhere Microsoft licensing (all or in part) in the form of Microsoft subscriptions that are not provided through Ricoh, the client can choose to transfer these licenses to Ricoh-provided subscriptions when the non-Ricoh subscriptions expire.

The client may also choose to transfer the non-Ricoh subscriptions to Ricoh prior to the expiration date, pending mutual agreement between the client, the legacy license provider, and Ricoh.

The client can also choose to retain the non-Ricoh subscriptions and renew them indefinitely.

Ricoh will charge an administrative fee for each Microsoft license required by Ricoh Work Anywhere not provided under a Ricoh-based subscription. The administrative fee will be charged to the client on a per license, per month basis. Ricoh will remove this fee if licenses from non-Ricoh subscriptions are transferred to Ricoh-based subscriptions.

Service Responsibilities

■ (or Ricoh)	Ricoh responsibility	+	add-on service or capability
Client (or blank)	client responsibility	$	additional fee may apply (determined by Ricoh)
▲	joint Ricoh / client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included

Any feature, function, service, or responsibility not expressly included or mentioned in this service description document is implied to be the client's responsibility.

Customer Success & Advisory Services

Goals:

- Provide client guidance and technological planning in regards to Ricoh services.
- Maximize customer's value realization of Ricoh solutions & services through adoption and utilization analysis.
- Align the customer's evolving needs with additional Ricoh solutions and service expansion.
- Provide quantifiable analytical assessment of the client's services journey, benchmarking and progress reporting based on Ricoh & vendor technology benchmarks and Best Practice standards.

	Basic (Included in RWA Small Business)	Advanced (Included in RWA & RWA Safe	Premium (Included in RWA Safe Plus)
Customer Success & Adoption			
Designated Customer Success Manager	■	■	■
Service Review Engagements	Annual	Quarterly	Monthly
Executive Business Review Engagements		Annual	Quarterly
Technology Advisory – Hybrid Work			
Designated Technology Advisor		■	■
Cloud & Hybrid Work Strategic Roadmapping Engagements		Semiannual	Quarterly
Service Experience Analytics			
Microsoft 365 Secure Score Review	Annual	Semiannual	Quarterly
Microsoft 365 Utilization Analytics Review		Semiannual	Quarterly
Microsoft 365 Adoption Score Review		Semiannual	Quarterly
Microsoft 365 Vulnerability Management Review			Quarterly
Ricoh Technology Health Score Update	Annual	Semiannual	Quarterly

Proactive Incident Detection & Response

Ricoh Work Anywhere Essentials does not include proactive monitoring, change event detection, or alerting capabilities for the Microsoft 365 solution.

Ricoh Work Anywhere Essentials relies on Microsoft's native capabilities and tools to detect and alert on potential Microsoft 365 platform performance degradation and outages.

Ricoh will endeavor to notify the client on any potential problems with Microsoft 365 as they are made aware to Ricoh. Such notifications are made to the client in email form and dependent of the successful function of Ricoh's and the client's email services.

Helpdesk & Support Services

Ricoh Helpdesk and Support services work with users to reactively troubleshoot and resolve incidents that occur through the normal usage of Ricoh-configured and supported features and functions.

Supported Microsoft 365 features are shown in Appendix A of this document.

	Basic (Included in RWA Small Business)	Advanced (Included in RWA & RWA Safe	Premium (Included in RWA Safe Plus)
Availability			
Hours of Operation – Client Representative Incident Submission *Eastern Standard Time (EST)*	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote
Hours of Operation – Client User Incident Submission *Eastern Standard Time (EST)*		7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote
Helpdesk Contact Options	Ricoh Portal Telephone Email Chat		
Incident Response & Resolution			
Reactive Incident first response troubleshooting & resolution	client	Ricoh	Ricoh
Reactive Incident escalation to Ricoh Specialist troubleshooting & resolution	client	Ricoh	Ricoh
Reactive Incident escalation to Microsoft Support troubleshooting & resolution	Ricoh	Ricoh	Ricoh
Problem Resolution			
Problem escalation to Ricoh Engineering	Ricoh	Ricoh	Ricoh
Ricoh Engineering problem review, troubleshooting, & resolution	Ricoh *($ may apply)*	Ricoh *($ may apply)*	Ricoh *($ may apply)*
Problem escalation to scoped and planned engineering engagement	$+	$+	$+

Solution Administration

Service solution administration is the day-to-day service activities surrounding individual users or devices engaged in using the service. These tasks typically do not require Ricoh Change Control review.

	Basic (Included in RWA Small Business)	Advanced (Included in RWA & RWA Safe	Premium (Included in RWA Safe Plus)
Availability			
Hours of Operation – Client Representative Request Submission *Eastern Standard Time (EST)*	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote
Contact Options		Ricoh Portal Telephone Email	
Microsoft Subscription Administration			
Microsoft 365 Subscription add/remove licenses	■	■	■
Microsoft Entra ID Identity & Access Administration			
Standard user account add/change/disable/remove *(see Appendix B for definition)*		■	■
Custom user account add/change/disable/remove		$	$
Guest user account add/change/disable/remove		■	■
User Account permissions add/change/remove		■	■
Group Membership add/change/remove		■	■
Multi Factor Authentication (MFA) self-service enrollment	user	user	user
Microsoft Exchange Online Administration			
Mail-enabled group membership add/change/remove		■	■
User mailbox add/change/disable/remove		■	■
Resource mailbox add/change/disable/remove		■	■
Distribution List membership add/change/remove		■	■
Contact add/change/remove		■	■
Microsoft Teams Administration			
Teams Site membership add/change/remove		■	■
Teams Site member permissions add/change/remove			■
Teams Channel membership add/change/remove		■	■
Teams Channel member permissions add/change/remove			■
Teams folder & file content add/change/remove/publish			
Teams content sharing permission add/change/remove			
Teams webinar & Live event setup & coordination			
Microsoft SharePoint Administration			
Folder/File add/change/remove			
Folder/File access permissions add/change/remove			
Folder/File sharing add/change/remove			
Folder/File restore previous version (in SharePoint)			
Administration Request Processing			
Included Service Administration Requests *(per 50 users)*	3 per month	5 per month	10 per month
Additional Service Administration Requests	*(per request $)*	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+	$+

Solution Configuration Management

Service solution configuration changes affect many users or the entire client organization. Therefore configuration change requests require formal Ricoh Change Control review and approval before being implemented.

Approved changes can include planning, testing, and phased or scheduled releases by Ricoh engineers; therefore configuration changes may require additional fees to implement depending on the scope and complexity of the change.

Note: Ricoh reserves the right to deny solution configuration change requests that negatively impact the Ricoh-configured SSRC performance and security. Other solution change requests may lie outside the managed scope of the Ricoh-configured SSRC and may be rejected or qualify as scoped & planned engineering engagements. Additional fees may apply.

	Basic (Included in RWA Small Business)	Advanced (Included in RWA & RWA Safe	Premium (Included in RWA Safe Plus)
Availability			
Hours of Operation – Client Representative Request Submission *Eastern Standard Time (EST)*	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote	7am – 7pm Monday – Friday Remote
Contact Options		Ricoh Portal Email	
Microsoft 365 Tenant Management			
Company Details changes	■	■	■
Billing Information changes	■	■	■
Customer Acceptance Information changes	■	■	■
Account Special Qualification changes *Client must qualify as per Microsoft criteria*	client	client	client
Customer Permissions changes	■	■	■
Admin Relationships changes	■	■	■
Microsoft Subscription Management			
Microsoft 365 Subscription creation	■	■	■
Microsoft 365 Subscription upgrade	■	■	■
Microsoft 365 Subscription renewal coordination	■	■	■
Microsoft 365 Subscription cancellation coordination	■	■	■
Microsoft Entra ID Management			
Ricoh Work Anywhere Identity SSRC configuration changes	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
Domain Name add/change/remove			$+
Entra ID Hybrid Sync configuration (cloud)	■	■	■
Entra ID Hybrid Sync agent install/uninstall/update *(Server / Delegated Domain administration access required)*			■
Single Sign-On (SSO) configuration	■	■	■
Tenant Administrator account add/change/disable/remove	■	■	■
Tenant Administrator RBAC permissions add/change/remove	■	■	■
Administrative Unit add/change/remove	■	■	■
Group add/change/remove	■	■	■

(Security, Dynamic, M365 groups)			
Group permissions add/change/remove *(Security, Dynamic, M365 groups)*	■	■	■
User Password Policy add/change/remove	■	■	■
Self-Service Password Reset configuration	■	■	■
Multi Factor Authentication Policy add/change/remove	■	■	■
Conditional Access Policy add/change/remove	■	■	■
Enterprise Application add/change/remove *Ricoh Work Anywhere Apps*	■	■	■
Enterprise Application add/change/remove *Other Apps*	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
App Registration add/change/remove *Ricoh Work Anywhere Apps*	■	■	■
App Registration add/change/remove *Other Apps*	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
External / Guest Account + Entitlement Management add/change/remove			$+
Privileged Identity Management changes	n/a	n/a	n/a
Exchange Online Management			
Mail Migration to/from separate mail platform	$+	$+	$+
Ricoh Work Anywhere Exchange SSRC configuration	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
Email Domain add/change/remove	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
DMARC, DKIM, SFP configuration	■	■	■
Mail-Enabled Security Group add/change/remove	■	■	■
Distribution List add/change/remove	■	■	■
Email Connector add/change/remove	■	■	■
Rules add/change/remove	■	■	■
Role Assignment Policy add/change/remove	■	■	■
Outlook Web Policy add/change/remove	■	■	■
Mobile Device Access Rule & Mailbox Policy add/change/remove	■	■	■
Public Folder add/change/remove	■	■	■
Public Mailbox add/change/remove	■	■	■
In-Place Archiving configuration	■	■	■
Federated Exchange configuration	$+	$+	$+
Hybrid Exchange configuration	$+	$+	$+
eDiscovery Mailbox Litigation Hold	■	■	■
eDiscovery Content Search			
eDiscovery Audit (Standard)			
Exchange Online Protection & Defender for Office 365 Management			
Ricoh Work Anywhere Exchange Protection SSRC configuration	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
Anti-Phishing Policy add/change/remove	■	■	■
Anti-Spam Policy add/change/remove	■	■	■
Anti-Malware Policy add/change/remove	■	■	■
Safe Attachment Policy add/change/remove	■	■	■
Safe Links Policy add/change/remove	■	■	■
Tenant Allow/Block List add/change/remove	■	■	■
Advanced Delivery Rules add/change/remove	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*
Enhanced Filtering Rules add/change/remove	■ *($ may apply)*	■ *($ may apply)*	■ *($ may apply)*

Quarantine Policy add/change/remove	■	■	■
Microsoft Teams Management			
Ricoh Work Anywhere Teams SSRC configuration	■	■	■
Teams Site add/change/remove			
Teams Channel add/change/remove			
Teams Channel member permissions add/change/remove			
Audio Conferencing Dial-In configuration	■	■	■
Teams Site / Channel 3rd-party application integration			
Microsoft SharePoint Online Management			
Ricoh Work Anywhere SharePoint SSRC configuration	n/a	n/a	n/a
Site/Collection/Library add/change/remove	n/a	n/a	n/a
Site/Collection/Library access control add/change/remove	n/a	n/a	n/a
Folder/ File external sharing	n/a	n/a	n/a
Microsoft OneDrive Management			
Ricoh Work Anywhere OneDrive SSRC configuration	■	■	■
Known Folder Redirection configuration	■	■	■
Microsoft Intune Application Management			
Ricoh Work Anywhere Intune Apps SSRC configuration	■	■	■
Microsoft App Deployment Policy add/change/remove	■	■	■
Microsoft App Protection Policy add/change/remove	■	■	■
Microsoft App Configuration Policy add/change/remove	■	■	■
Productivity App Suite Deployment Policy add/change/remove		■	■
Productivity App Protection Policy add/change/remove		■	■
Productivity App Configuration Policy add/change/remove		■	■
Intune Company Portal App add/change/remove			■
Microsoft Score Management			
Microsoft 365 Secure Score: Pre-Implementation Reference	■	■	■
Microsoft 365 Secure Score: Pre-Implementation Baseline	■	■	■
Microsoft 365 Secure Score: Update	Annual	Semiannual	Quarterly
Microsoft Adoption Score: Update			
Microsoft Vulnerability Score: Update			$
Microsoft Compliance Score: Update			$
Configuration Change Request Processing			
Included Configuration Change Requests *(per 50 users)*	3 per month	3 per month	3 per month
Additional Configuration Change Requests	*(per request $)*	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+	$+

Appendix A: Supported Microsoft 365 Features: Ricoh Work Anywhere Essentials

The below list represents the full Microsoft 365 feature stack plus related Ricoh-provided solution features. Different components of Ricoh Work Anywhere will reference different portions of the list and will be reflected in each component's separate service description document.

The list below represents supported features for Ricoh Work Anywhere Essentials.

Note: features may change as per Microsoft discretion. Always refer to Microsoft's latest M365 feature definitions for the plans defined for Ricoh Work Anywhere.

■ (or Ricoh)	Ricoh responsibility	$	additional fee may apply (determined by Ricoh)
Client (or blank)	client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included
+	add-on service or capability		

	Basic (Included in RWA Small Business)	Advanced (Included in RWA & RWA Safe	Premium (Included in RWA Safe Plus)
Microsoft 365 Application Support			
Microsoft Office 365 (Web)	■	■	■
Microsoft Office 365 (Desktop)	■	■	■
Microsoft Office 365 (Mobile)			
Visio for the Web		■	■
Microsoft Loop components, pages, and workspaces		■	■
Microsoft ClipChamp		■	■
Microsoft Editor		■	■
Multilingual Office Apps Interface			
Microsoft Office Shared Computer Activation			■
Microsoft Exchange Online Support			
User, Resource, Inactive Mailboxes	■	■	■
Distribution Lists & Contacts	■	■	■
Calendars	■	■	■
Public Folders & Mailboxes	■	■	■
In-Place Archiving & Auto-Expanding Archive	■	■	■
Microsoft Shifts			
Microsoft Bookings			
Microsoft Teams			
Teams Online Chat	■	■	■
Teams Online Meetings	■	■	■
Teams Live Events			
Teams Webinars (created & coordinated by customer employees)	■	■	■
Teams Audio Conferencing	■	■	■
Teams Avatars			
Teams Phone			
Teams File Sharing & Co-Authoring	■	■	■
Microsoft SharePoint Online, OneDrive & Yammer			
Microsoft SharePoint Online Sites, Lists, Libraries			
Microsoft OneDrive & Known Folder Redirection	■	■	■
Microsoft Viva Connections			

Microsoft Viva Engage			
Microsoft Yammer			
Microsoft 365 Knowledge, Insights, & Content			
Microsoft Graph API			
Microsoft Search	■	■	■
Microsoft Stream			
Microsoft Forms	■	■	■
Microsoft Lists	■	■	■
Microsoft Delve	■	■	■
Expertise identification			
Document Understanding/Form Processing			
Access Content Centers			
Document Understanding/Form Processing Metadata Viewing			
Microsoft Viva Insights			■
Microsoft Viva Learning			
Microsoft 365 Analytics & Insights			
Microsoft Secure Score	See Solution Management	See Solution Management	See Solution Management
Microsoft Adoption Score	See Solution Management	See Solution Management	See Solution Management
Microsoft Compliance Score	See Solution Management	See Solution Management	See Solution Management
Microsoft Vulnerability Score	See Solution Management	See Solution Management	See Solution Management
Microsoft 365 Project & Task Management			
Microsoft Planner	■	■	■
Microsoft To-Do	■	■	■
Automation & App Development			
Microsoft Power Apps for Microsoft 365			
Microsoft Power Automate for Microsoft 365			
Microsoft CoPilot Studio for Teams			
Dataverse for Teams			
Microsoft 365 Copilot			
Microsoft Copilot (Edge Browser)			
Microsoft Copilot for Office Applications			
Microsoft Copilot for Teams			
Microsoft Copilot Studio			
Microsoft 365 Endpoint & App Management			
General			
Intune Endpoint Device Enrollment & Restriction policies			
Intune Endpoint Device Conditional Access policies			
Intune Endpoint Device Compliance policies			
Intune Endpoint Windows Hello Policies			
Windows 10+ OS Endpoints			
Intune Windows Endpoint Configuration Profiles			
Intune Windows Endpoint Security Baselines			
Intune Update Rings (Ricoh standard configuration)			
Intune Update Rings (custom configuration)			
Intune Quality Updates for Windows 10+ Endpoint OS			
Intune Feature Upgrades for Windows 10+ Endpoint OS			
Windows 365 Cloud PC Endpoint			
Intune AutoPilot Profiles: Windows Endpoint (Ricoh standard configuration)			
Intune AutoPilot Profiles: Windows Endpoint (custom configuration)			
macOS Endpoints			
Intune macOS Enrollment Configuration			
Intune macOS Endpoint Configuration Profiles			

Intune macOS Compliance Policies			
Intune macOS Endpoint Update Profiles			
Mobile Endpoints - Android			
Intune App Configuration policies: Mobile M365 Apps			
Intune App Protection policies: Mobile M365 Apps			
Intune Mobile Device Management polices			
Intune iOS provisioning profiles configuration			
Mobile Endpoints – iOS/iPadOS			
Intune App Configuration policies: Mobile M365 Apps			
Intune App Protection policies: Mobile M365 Apps			
Intune Mobile Device Management polices			
Intune iOS provisioning profiles configuration			
Applications			
Intune Company Portal			
Intune App Configuration policies: Windows Endpoint Office Apps	■	■	■
Intune App Configuration policies: Windows Endpoint Ricoh Productivity Apps bundle		■	■
Office Apps Cloud Policy			
Microsoft 365 Threat Protection			
Microsoft Defender for Business			
Microsoft Defender for Endpoint Plan 1			
Microsoft Defender for Endpoint Plan 2	n/a	n/a	n/a
Microsoft Defender for Office 365 Plan 1			
Microsoft Defender for Office 365 Plan 2	n/a	n/a	n/a
Microsoft Defender for Identity	n/a	n/a	n/a
Microsoft Defender Application Guard for Office 365	n/a	n/a	n/a
Microsoft Defender Application Guard for Edge			
Microsoft Defender Antimalware			
Microsoft Defender Firewall			
Microsoft Defender Exploit Guard	■	■	■
Microsoft Defender Credential Guard	■	■	■
Microsoft Defender for IoT	n/a	n/a	n/a
BitLocker			
BitLocker To Go			
Windows Information Protection			
Safe Documents	n/a	n/a	n/a
Ricoh Threat Protection			
Ricoh Endpoint Protection: Windows Endpoint standard anti-malware			
Ricoh Endpoint Protection: Managed Security *Windows 10 endpoint Managed Detection (MDR) & Response + 24x7 SOC*			
Microsoft Cloud Access Security Broker (CASB)			
Microsoft Defender Cloud Apps	n/a	n/a	n/a
Microsoft Defender for Cloud App Discovery			$+
App Governance in Defender for Cloud Apps	n/a	n/a	n/a
Office 365 Cloud App Security	n/a	n/a	n/a
Microsoft 365 Identity & Access Management			
Azure Active Directory Domains	■	■	■
Azure Active Directory Administrative Units	■	■	■
Azure Active Directory User & Guest Accounts (standard)	■	■	■
Azure Active Directory User & Guest Accounts (custom)			
Azure Active Directory Registered Device Accounts			■
Azure Active Directory Azure AD joined Device Accounts	■	■	■
Hybrid Active Directory joined Device Accounts			
Azure Active Directory Registered Applications			■
Azure Active Directory Service Principals			■
Azure Active Directory Managed Identities (System & User assigned)			■

Azure Active Directory External Identities			
Azure Active Directory RBAC Roles & Administrators	■	■	■
Azure Active Directory Security Groups	■	■	■
Azure Active Directory Dynamic Groups	■	■	■
Microsoft 365 Groups	■	■	■
Azure Active Directory Identity Governance	n/a	n/a	n/a
Azure Active Directory Application Proxy			
Self Service Password Reset	■	■	■
Multi Factor Authentication	■	■	■
Conditional Access	■	■	■
Risk Based Conditional Access/Identity Protection	n/a	n/a	n/a
Verifiable Credentials / Decentralized Identity	n/a	n/a	n/a
Privileged Identity Management	n/a	n/a	n/a
Access Reviews	n/a	n/a	n/a
Entitlement Management	n/a	n/a	n/a
DirectAccess			
Single Sign-On (SSO)	■	■	■
Windows Hello for Business			
Microsoft Advanced Threat Analytics			
Microsoft 365 Information Protection			
Microsoft Information Protection Plan 1 settings & policies configuration			
Microsoft Information Protection Plan 2 settings & policies configuration	n/a	n/a	n/a
Manual, default, & mandatory sensitivity labels			
Automatic sensitivity labels	n/a	n/a	n/a
Manual sensitivity labels for Teams Meetings	n/a	n/a	n/a
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive	n/a	n/a	n/a
Sensitivity labels based on advanced classification (ML, EDM)	n/a	n/a	n/a
Sensitivity labeling for containers in Microsoft 365			
Data Loss Prevention (DLP) for emails and files		■	■
Basic Office Message Encryption	■	■	■
Advanced Office Message Encryption	n/a	n/a	n/a
Customer Key	n/a	n/a	n/a
Personal Data Encryption			
Windows Information Protection			
Microsoft 365 Data Lifecycle Management			
Manual retention labels			$+
Basic org-wide or location-wide retention policies			$+
Rules-based automatic retention policies	n/a	n/a	n/a
Machine Learning-based retention	n/a	n/a	n/a
Teams message retention policies	n/a	n/a	n/a
Records Management	n/a	n/a	n/a
Microsoft 365 eDiscovery & Auditing			
Content Search			
Standard eDiscovery including Hold and Export			
Litigation Hold		■	■
Premium eDiscovery	n/a	n/a	n/a
Standard Audit			
Premium Audit	n/a	n/a	n/a
Microsoft 365 Insider Risk Management			
Insider Risk Management	n/a	n/a	n/a
Communication Compliance	n/a	n/a	n/a
Information Barriers	n/a	n/a	n/a
Customer Lockbox	n/a	n/a	n/a
Privileged Access Management	n/a	n/a	n/a
Microsoft Universal Print			

Universal Print configuration for UP-Ready printers Controlled in the M365 cloud			
Universal Print configuration for non UP-Ready printers Requires UP Connector app installed on local workstation or server			

Appendix B: Standard User Account Administration

Ricoh defines standard User Account Administration as the following list of activities:

- **User account creation:**
    - The account will be created in Entra ID based on these principal information elements:
        - User's first, middle, and last name
        - User's designated department in the customer's organization
        - User's primary and alias email domain names
        - User's membership in Entra ID Groups
        - User's assigned workstation
        - User's enrollment in Ricoh Desktop Anywhere managed cloud PC services
        - User's enrollment in Intune Mobile Application Management (MAM) or Mobile Device Management (MDM) services
        - User's membership in Intune Application Management Groups – this determines applications installed for user via Intune (must be enrolled in Managed Windows Endpoint or Desktop Anywhere services)
        - User's designated Microsoft subscription type
        - Other data may be included in the request submission that helps further define the user account requirements.
    - The user's account will be created in the client's standard naming format.
    - The user's account will be provisioned with the proper Microsoft licensing.
    - The user's account will be added to the appropriate Entra ID Groups.
    - The user's mailbox will be created with standard settings.
    - Configuration policies will automatically be assigned to the user's account. These policies will determine the level of access, assigned applications, and other functional capabilities of the user.
    - The user will need to register any personal devices into MFA.
- **User account changes:**
    - Name changes
    - Email and alias domain name changes
    - Group membership changes
    - Services enrollment changes
    - Microsoft licensing changes
    - Workstation assignment changes
- **User account disablement:**

- Requested submitted by designated client PoC with the following data:
  - User account name
  - Desired time of disablement
  - Deferred account access to another person (provide name)
  - Set account retirement date:
    - Choice of 30/60/90/180 day timeline for account retirement
- Disablement conducted in Entra ID:
  - User account forced password reset
  - Unassign/Disable user's designated managed Windows endpoint(s)
  - Assign deferred admin access (if defined by PoC)

- **User account retirement:**
  - Occurs as per disablement timeline specification
  - Target account data and email migrations are conducted by deferred account administrator prior to retirement date (see account disablement)
  - On Target Date:
    - Retirement conducted in Entra ID
    - Delete user's Desktop Anywhere cloud PC instance (if applicable)
    - Email mailbox transition from User Mailbox to Resource Mailbox
    - Unassign user account licensing
    - Delete user account

Note: Any user account administration workflow requirements beyond this scope are considered "custom". Ricoh will apply a feed for custom user account administration.

Windows Endpoint Service Description for Ricoh Work Anywhere

Overview

What is Ricoh Work Anywhere Windows Endpoint?

Ricoh Work Anywhere Windows Endpoint is designed to address the needs of Windows Endpoint Operating System (OS) management and device support:

- Standardized policy-driven Windows Endpoint OS and device configuration.
- Windows Endpoint OS security & encryption.
- Windows OS Quality and Feature Upgrade management.
- Windows Endpoint reactive device support.
- Automated self-service Windows Endpoint deployment.
- Automated Windows Endpoint reset & re-assignment.

Ricoh Work Anywhere Windows Endpoint Service Tiers

There are two (2) tiers of service for Ricoh Work Anywhere Windows Endpoint:

OS Protect	Managed Device
Included in RWA Small Business Bundle Budget-oriented for customers who seek to control cost by adopting a shared responsibility model for support and management of Windows Endpoints in the customer's organization. This level of service places the responsibilities of endpoint Operating System & device support, deployment, tracking, re-assignment & retirement operations with the client's in-house IT organization. The Client Representative can escalate Windows OS incidents to Ricoh specialists for further troubleshooting & resoltion, and Ricoh escalation to Microsoft if required. Ricoh provides Microsoft 365 device policy configuration management, Application policy management for Office 365 and Ricoh Productivity Suite app deployments to Windows Endpoints, Endpoint anti-malware, and Endpoint enrollment in Ricoh's Windows Endpoint management platform. Ricoh can provide OS inventory reports.	**Included in RWA, RWA Safe and RWA Safe Plus Bundles** Designed for companies that seek provider-operated solution and services to reduce in-house IT workloads and burdens. This tier of service includes all of the value of Basic, plus the following: • Ricoh is responsible for Windows OS & device support. End Users and Client Representatives may report support incidents to Ricoh directly for incident response, escalation, and resolution. • Ricoh is responsible for new Windows Endpoint deployment, and existing Endpoint reset & re-assignment requests made by the Client Representative. • Device inventory reports.

Service Requirements

Ricoh Work Anywhere
The client's end users must be enrolled in a Ricoh Work Anywhere service bundle that contains this service, at a tier level defined by the Work Anywhere service bundle definition.

Windows Operating System
Windows Endpoint Operating Systems must meet these requirements:

- Company-provisioned endpoint for business use (personal endpoints not supported)
- Windows OS version 10 or higher
- Windows OS type must be Pro or Enterprise
- Windows OS version & build number must be within Microsoft's defined active date range of supported Operating Systems (see Microsoft documentation on supported Windows OS versions)
- Windows OS licensing is provided to the endpoint via OEM associated with the device purchase; provisioned by a valid client license purchase or subscription-based plan provided by Microsoft or valid reseller.
- The Windows Endpoint is fully joined to Microsoft 365 Entra ID
    - Hybrid Join is not supported
    - See Microsoft documentation for detail on fully-joined and hybrid-joined Windows Endpoints

Windows Endpoint Devices
The device hardware must meet these requirements:

- Company-provisioned endpoint for business use (personal endpoints not supported)
- Device is from a Ricoh-recognized manufacturer
- Device model must meet Microsoft hardware requirements for Microsoft 365 Business Premium capabilities, or higher
    - See Microsoft documentation for M365 Business Premium hardware requirements
- Device model must be within the manufacturer's active product support lifecycle:
    - The model cannot be considered End of Life

Optional but preferred for best service experience:

- The device is covered by the manufacturer's hardware warranty (or 3rd-party equivalent)
- The device is covered by the manufacturer's accidental damage & theft replacement plan (or 3rd-party equivalent)

Microsoft Licensing
The end users utilizing these services must be licensed as per the appropriate Microsoft subscription requirements for Work Anywhere services.

Ricoh Service Delivery

Ricoh may install software tools and utilities on the Windows Endpoint for the purposes of monitoring, reporting, or facilitating service delivery. Ricoh may choose to upgrade, change or discontinue use of these applications at any time. Customer refusal, removal, or other conditions beyond Ricoh's ability to affect that prevent these application installations and upgrades impacts Ricoh's ability to deliver service, which may relieve Ricoh of service responsibilities for the affected Windows Endpoint(s).

Ricoh service includes administrative access to the Windows Endpoint(s) for the purpose of service delivery as defined in this document. Ricoh's access utilizes Local Administrator accounts on each Endpoint created exclusively for Ricoh use while the client is enrolled in this service. Ricoh administrative account access credentials are reserved for Ricoh's knowledge and use only. No other party will have access to these accounts or credentials.

Ricoh's ability to troubleshoot device network and Internet connectivity issues depends on the type of network the device is connected to, and if that network is managed by Ricoh (or not). Ricoh has the greatest chance of resolving device connectivity issues when the device is connected to the company network that is also managed by Ricoh. Ricoh cannot troubleshoot:

- Devices connected to non-company networks
- Devices connected to company networks not managed by Ricoh
- Devices connected to the Internet via cellular service providers
- Devices connected to public networks

Service Responsibilities

■ (or Ricoh)	Ricoh responsibility	+	add-on service or capability
Client (or blank)	client responsibility	$	additional fee may apply (determined by Ricoh)
▲	joint Ricoh / client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included

Any feature, function, service, or responsibility not expressly included or mentioned in this service description document is implied to be the client's responsibility.

Customer Success & Advisory Services

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description documentation for general service entitlements and availability.

In addition, these service entitlements apply for this service.

	OS Protect (Included in RWA Small Business)	Managed Endpoint (Included in RWA, RWA Safe, and RWA Safe Plus
Service Experience Analytics		
Microsoft Windows Endpoint Inventory: Operating System (OS) - OS type, version, & build - Last system check-in date & time - Last logged in user name	■	■
Microsoft Windows Endpoint Inventory: Device - Name - Network Address - Manufacturer - Model - Asset Tag / Serial Number - Purchase Date - Warranty Date		■

Proactive Incident Detection & Response

Ricoh Work Anywhere Windows Endpoint collects:

- Windows Endpoint OS & device informational and performance data for use in providing reactive incident support service delivery
- Windows system and security log events
- Installed applications

Ricoh Work Anywhere Windows Endpoint does not collect:

- User personal information (other than logon name)
- User passwords or biometric identification data
- User Internet browsing activity or history
- User general activity
- Screenshots
- Application activity (other than Microsoft event logs)
- Specific folder or file names or content
- Endpoint location
- Endpoint keyboard input
- Endpoint mouse or pointer input
- Endpoint camera or microphone inputs
- Scan/Print activity or content

Ricoh Work Anywhere Windows Endpoint does not include change event detection or alerting services.

Helpdesk & Support Services

Ricoh Helpdesk and Support services work with users to reactively troubleshoot and resolve incidents that occur through the normal usage of Ricoh-configured and supported features and functions.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, supported features for this service are shown in Appendix A of this document.

Solution Administration

Service solution administration is the day-to-day service activities surrounding individual users or devices engaged in using the service. These tasks typically do not require Ricoh Change Control review.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, these service entitlements apply.

	OS Protect (Included in RWA Small Business)	Managed Endpoint (Included in RWA, RWA Safe, and RWA Safe Plus
Windows Endpoint Administration		
Ad Hoc Azure AD Join/Unjoin total per month	client	■
Ad Hoc Hybrid AD Join/Unjoin total per month	client	■
Ad Hoc Azure AD Registered Device total per month	client	■
Ad Hoc Windows Endpoint disable operations total per month	client	■
Ad Hoc remote Windows Endpoint reset total per month • *Reset via Microsoft Autopilot* • *Reset to Ricoh standard configuration*	client	■
Ad Hoc remote Windows Endpoint reassignment total per month • *Reset via Microsoft Autopilot* • *Reset to Ricoh standard configuration* • *User / device group reassignment as per request*	client	■
Ad Hoc Windows Endpoint reassignment (device packaging, relocation & end user delivery)	client	client
Ad Hoc Bitlocker decrypt / encrypt operations & key recovery total per month	client	■
Administration Request Processing		
Included Service Administration Requests *(per 50 users)*	n/a	5 per month
Additional Service Administration Requests	n/a	*(per request $)*
Bulk Request Processing	n/a	$+

Solution Configuration Management

Service solution configuration changes affect many users or the entire client organization. Therefore configuration change requests require formal Ricoh Change Control review and approval before being implemented.

Approved changes can include planning, testing, and phased or scheduled releases by Ricoh engineers; therefore configuration changes may require additional fees to implement depending on the scope and complexity of the change.

Note: Ricoh reserves the right to deny solution configuration change requests that negatively impact the Ricoh-configured SSRC performance and security. Other solution change requests may lie outside the managed scope of the Ricoh-configured SSRC and may be rejected or qualify as scoped & planned engineering engagements. Additional fees may apply.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, these service entitlements apply.

	OS Protect (Included in RWA Small Business)	Managed Endpoint (Included in RWA, RWA Safe, and RWA Safe Plus
Windows Endpoint Management		
General		
Intune Conditional Access Policy add/change/remove	■	■
Intune Compliance Policy add/change/remove	■	■
Intune Enrollment & Restriction Policy add/change/remove	■	■
Intune Enrollment Windows Hello Policy add/change/remove	■	■
Intune Enrollment Endpoint User Limit Policy add/change/remove	■	■
Windows Endpoints		
Intune Windows Endpoint Configuration Profile add/change/remove	■	■
Intune Windows Endpoint Security Baseline add/change/remove	■	■
Intune Windows Endpoint Autopilot Configuration • *Ricoh Standard Configuration*		■ *($ may apply)*
MacOS Endpoints		
Intune Apple Enrollment (Program Tokens)		
Intune Apple Bulk Enrollment (Apple Configurator)		
Intune macOS Device Configuration Profile add/change/remove		
Intune macOS Compliance Policy add/change/remove		
Configuration Change Request Processing		
Included Configuration Change Requests *(per 50 users)*	3 per month	3 per month
Additional Configuration Change Requests	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+

Windows Endpoint Lifecycle Management

Lifecycle Management consists of activities regularly conducted to keep a system, device, or service current and up-to-date, or to make service course corrections based on changing technology requirements.

Lifecycle Management begins with an observed Lifecycle Event which is usually announced and scheduled in advance by a solution or service provider. Some are regularly scheduled repeat activities, others are one-time changes.

Lifecycle Events need to be assessed, tested, and approved before integrating with a managed service. Events may constitute minor or major changes to service architecture and incur costs to both Ricoh and the client.

Rich will endeavor to maintain foresight of upcoming Lifecycle Events and regularly-scheduled Events, and plan, validate, and test prior to general application to our service offerings.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

Note: Ricoh reserves the right to deny Lifecycle Events that negatively impact the Ricoh-configured SSRC performance and security. Other Events may lie outside the managed scope of the Ricoh-configured SSRC and may be rejected or qualify as scoped & planned engineering engagements.

	OS Protect (Included in RWA Small Business)	Managed Endpoint (Included in RWA, RWA Safe, and RWA Safe Plus
Windows Endpoint Lifecycle Management		
OS Lifecycle Management		
Microsoft Windows Quality Updates (standard scheduled)	■	■
Microsoft Windows Quality Updates (ad hoc per Ricoh discretion)	■	■
Microsoft Windows Quality Updates (custom scheduled)	$	$
Microsoft Windows Feature Upgrades	■	■
Microsoft 365 Applications		
Office 365 Application Updates & Upgrades	Microsoft	Microsoft
Microsoft Teams Updates & Upgrades	Microsoft	Microsoft
Microsoft Office Updates & Upgrades	Microsoft	Microsoft
Microsoft 365 Apps Updates & Upgrades	Microsoft	Microsoft
Ricoh Productivity App Suite Updates	Ricoh *(as required)*	Ricoh *(as required)*
Windows Endpoint Devices		
New Endpoint Deployment: Standard Purchased via Ricoh • *Purchase Work Order required*		Standard Autopilot *(see Appendix B)*
New Endpoint Deployment: Standard Purchased via others • *Service Work Order required*		Standard Autopilot *(see Appendix B)* *($ fee applies)*
New Endpoint Deployment: Custom • *Service Work Order required*		Autopilot *(see Appendix B)* *($ fee applies)*
Windows Endpoint Device BIOS updates		As required for Support *($ fee may apply)*
Windows Endpoint System Firmware updates		As required for Support *($ fee may apply)*
Windows Endpoint Device Driver updates		As required for Support

		($ fee may apply)
Windows Endpoint Device proactive mfgr. EOL tracking & replacement planning		
Windows Endpoint Device mfgr. warranty/support expiration tracking		
Windows Endpoint Device mfgr. warranty/support renewal management		
Windows Endpoint Device retirement: Standard		Standard Autopilot *(see Appendix B)*
Windows Endpoint Device retirement: Custom		Autopilot *(see Appendix B)* *($ fee applies)*
Windows Endpoint Device delivery / return coordination	client	client
Windows Endpoint Device delivery / return shipping fees	client	client
Configuration Change Request Processing		
Included Configuration Change Requests *(per 50 users)*	3 per month	3 per month
Additional Configuration Change Requests	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+

Appendix A: Supported Service Features: Work Anywhere Windows Endpoint

The below list represents the **full** Microsoft 365 feature stack plus related Ricoh-provided solution features. Different components of Ricoh Work Anywhere will reference different portions of the list and will be reflected in each component's separate service description document.

The list below represents supported features for Ricoh Work Anywhere Windows Endpoint.

Note: features may change as per Microsoft discretion. Always refer to Microsoft's latest M365 feature definitions for the plans defined for Work Anywhere.

■ (or Ricoh)	Ricoh responsibility	$	additional fee may apply (determined by Ricoh)
Client (or blank)	client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included
+	add-on service or capability		

	OS Protect (Included in RWA Small Business)	Managed Endpoint (Included in RWA, RWA Safe, and RWA Safe Plus
Microsoft 365 Application Support		
Microsoft Office 365 (Web)		
Microsoft Office 365 (Desktop)		
Microsoft Office 365 (Mobile)		
Visio for the Web		
Microsoft Loop components, pages, and workspaces		
Microsoft ClipChamp		
Microsoft Editor		
Multilingual Office Apps Interface		
Microsoft Office Shared Computer Activation		
Microsoft Exchange Online Support		
User, Resource, Inactive Mailboxes		
Distribution Lists & Contacts		
Calendars		
Public Folders & Mailboxes		
In-Place Archiving & Auto-Expanding Archive		
Microsoft Shifts		
Microsoft Bookings		
Microsoft Teams		
Teams Online Chat		
Teams Online Meetings		
Teams Live Events		
Teams Webinars (created & coordinated by customer employees)		
Teams Audio Conferencing		
Teams Avatars		
Teams Phone		
Teams File Sharing & Co-Authoring		
Microsoft SharePoint Online, OneDrive & Yammer		
Microsoft SharePoint Online Sites, Lists, Libraries		
Microsoft OneDrive & Known Folder Redirection		
Microsoft Viva Connections		
Microsoft Viva Engage		
Microsoft Yammer		
Microsoft 365 Knowledge, Insights, & Content		
Microsoft Graph API		
Microsoft Search		

Microsoft Stream		
Microsoft Forms		
Microsoft Lists		
Microsoft Delve		
Expertise identification		
Document Understanding/Form Processing		
Access Content Centers		
Document Understanding/Form Processing Metadata Viewing		
Microsoft Viva Insights		
Microsoft Viva Learning		
Microsoft 365 Analytics & Insights		
Microsoft Secure Score		
Microsoft Adoption Score		
Microsoft Compliance Score		
Microsoft Vulnerability Score		
Microsoft 365 Project & Task Management		
Microsoft Planner		
Microsoft To-Do		
Automation & App Development		
Microsoft Power Apps for Microsoft 365		
Microsoft Power Automate for Microsoft 365		
Microsoft CoPilot Studio for Teams		
Dataverse for Teams		
Microsoft 365 Copilot		
Microsoft Copilot (Edge Browser)		
Microsoft Copilot for Office Applications		
Microsoft Copilot for Teams		
Microsoft Copilot Studio		
Microsoft 365 Endpoint & App Management		
General		
Intune Endpoint Device Enrollment & Restriction policies	■	■
Intune Endpoint Device Conditional Access policies	■	■
Intune Endpoint Device Compliance policies	■	■
Intune Endpoint Windows Hello Policies	■	■
Windows 10+ OS Endpoints		
Intune Windows Endpoint Configuration Profiles	■	■
Intune Windows Endpoint Security Baselines	■	■
Intune Update Rings (Ricoh standard configuration)		
Intune Update Rings (custom configuration)		
Intune Quality Updates for Windows 10+ Endpoint OS	■	■
Intune Feature Upgrades for Windows 10+ Endpoint OS	■	■
Windows 365 Cloud PC Endpoint		
Intune AutoPilot Profiles: Windows Endpoint (Ricoh standard configuration)		■
Intune AutoPilot Profiles: Windows Endpoint (custom configuration)		$
macOS Endpoints		
Intune macOS Enrollment Configuration		
Intune macOS Endpoint Configuration Profiles		
Intune macOS Compliance Policies		
Intune macOS Endpoint Update Profiles		
Mobile Endpoints - Android		
Intune App Configuration policies: Mobile M365 Apps		
Intune App Protection policies: Mobile M365 Apps		
Intune Mobile Device Management polices		
Intune iOS provisioning profiles configuration		
Mobile Endpoints – iOS/iPadOS		
Intune App Configuration policies: Mobile M365 Apps		
Intune App Protection policies: Mobile M365 Apps		
Intune Mobile Device Management polices		
Intune iOS provisioning profiles configuration		

Applications		
Intune Company Portal	■	■
Intune App Configuration policies: Windows Endpoint Office Apps	■	■
Intune App Configuration policies: Windows Endpoint Ricoh Productivity Apps bundle		■
Intune App Configuration policies: Mobile Office Apps		
Office Apps Cloud Policy		
Windows Endpoint Devices		
Company owned & provisioned endpoint devices: OS	■	■
Company owned & provisioned devices: Hardware		■
Personal devices		
Endpoint Domain Enrollment	Entra ID Joined	Entra ID Joined
Endpoint peripheral devices, docking / charging equipment, external monitors, or other wired / wireless connected devices		
Endpoint Network & Internet connectivity		■ *(on-board NIC / WNIC functionality only)*
Endpoint device OS malfunction	■	■
Endpoint device hardware malfunction		■
Endpoint device failed hardware replacement coordination		
Endpoint device proactive hardware replacement coordination		
Microsoft 365 Threat Protection		
Microsoft Defender for Business		
Microsoft Defender for Endpoint Plan 1		
Microsoft Defender for Endpoint Plan 2	n/a	n/a
Microsoft Defender for Office 365 Plan 1		
Microsoft Defender for Office 365 Plan 2	n/a	n/a
Microsoft Defender for Identity	n/a	n/a
Microsoft Defender Application Guard for Office 365	n/a	n/a
Microsoft Defender Application Guard for Edge		
Microsoft Defender Antimalware		
Microsoft Defender Firewall		
Microsoft Defender Exploit Guard		
Microsoft Defender Credential Guard		
Microsoft Defender for IoT	n/a	n/a
BitLocker		
BitLocker To Go		
Windows Information Protection		
Safe Documents	n/a	n/a
Ricoh Threat Protection		
Ricoh Endpoint Protection: Windows Endpoint standard anti-malware	■	■
Ricoh Endpoint Protection: Managed Security *Windows 10 endpoint Managed Detection (MDR) & Response + 24x7 SOC*	+	+
Microsoft Cloud Access Security Broker (CASB)		
Microsoft Defender Cloud Apps	n/a	n/a
Microsoft Defender for Cloud App Discovery		
App Governance in Defender for Cloud Apps	n/a	n/a
Office 365 Cloud App Security	n/a	n/a
Microsoft 365 Identity & Access Management		
Azure Active Directory Domains		
Azure Active Directory Administrative Units		
Azure Active Directory User & Guest Accounts (standard)		
Azure Active Directory User & Guest Accounts (custom)		
Azure Active Directory Registered Device Accounts		
Azure Active Directory Azure AD Joined Device Accounts		■
Hybrid Active Directory Joined Device Accounts		
Azure Active Directory Registered Applications		■
Azure Active Directory Service Principals		
Azure Active Directory Managed Identities (System & User assigned)		
Azure Active Directory External Identities		

Azure Active Directory RBAC Roles & Administrators		
Azure Active Directory Security Groups		
Azure Active Directory Dynamic Groups		
Microsoft 365 Groups		
Azure Active Directory Identity Governance	n/a	n/a
Azure Active Directory Application Proxy		
Self Service Password Reset		
Multi Factor Authentication		
Conditional Access	■	■
Risk Based Conditional Access/Identity Protection	n/a	n/a
Verifiable Credentials / Decentralized Identity	n/a	n/a
Privileged Identity Management	n/a	n/a
Access Reviews	n/a	n/a
Entitlement Management	n/a	n/a
DirectAccess		
Single Sign-On (SSO)		
Windows Hello for Business	■	■
Microsoft Advanced Threat Analytics		
Microsoft 365 Information Protection		
Microsoft Information Protection Plan 1 settings & policies configuration		
Microsoft Information Protection Plan 2 settings & policies configuration	n/a	n/a
Manual, default, & mandatory sensitivity labels		
Automatic sensitivity labels	n/a	n/a
Manual sensitivity labels for Teams Meetings	n/a	n/a
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive	n/a	n/a
Sensitivity labels based on advanced classification (ML, EDM)	n/a	n/a
Sensitivity labeling for containers in Microsoft 365		
Data Loss Prevention (DLP) for emails and files		
Basic Office Message Encryption		
Advanced Office Message Encryption	n/a	n/a
Customer Key	n/a	n/a
Personal Data Encryption		
Windows Information Protection		
Microsoft 365 Data Lifecycle Management		
Manual retention labels		
Basic org-wide or location-wide retention policies		
Rules-based automatic retention policies	n/a	n/a
Machine Learning-based retention	n/a	n/a
Teams message retention policies	n/a	n/a
Records Management	n/a	n/a
Microsoft 365 eDiscovery & Auditing		
Content Search		
Standard eDiscovery including Hold and Export		
Litigation Hold		
Premium eDiscovery	n/a	n/a
Standard Audit		
Premium Audit	n/a	n/a
Microsoft 365 Insider Risk Management		
Insider Risk Management	n/a	n/a
Communication Compliance	n/a	n/a
Information Barriers	n/a	n/a
Customer Lockbox	n/a	n/a
Privileged Access Management	n/a	n/a
Microsoft Universal Print		
Universal Print configuration for UP-Ready printers Controlled in the M365 cloud		
Universal Print configuration for non UP-Ready printers Requires UP Connector app installed on local workstation or server		

Appendix B: Standard Windows Endpoint Administration

Ricoh defines standard Windows Endpoint Administration as the following list of activities:

- **New Endpoint Provisioning:**
    - New Windows Endpoints are purchased by the client through Ricoh providing the following information:
        - Endpoint device make / model
        - Endpoint device hardware configuration
        - End User name
        - End user shipping address
    - The Endpoint is configured by the manufacturer and shipped directly to the end user's address.
    - Ricoh will enroll the new device the new Endpoint in Microsoft Autopilot and Ricoh's standardized Autopilot profile and Intune policies will apply.
    - The Client will coordinate all notification and instruction with the end user prior to the scheduled delivery date.
    - The device is received by the end user and setup as per instruction.
    - If the user has an existing Endpoint, Ricoh will reset that endpoint at the end of the new Endpoint setup.

- **Endpoint Reset:**
    - Endpoint Reset will be conducted remotely upon Client Representative request of if required for Support troubleshooting.
    - Ricoh will conduct the reset action via Autopilot at a determined date / time.
    - The Endpoint will be reverted to Factory condition as a result of the reset.

- **Endpoint Reassignment:**
    - Upon request of the Client Representative, an Endpoint can be reassigned to a different end user.
    - This action is typically paired with new Endpoint provisioning for a given user.
    - Ricoh will execute provisioning and reset actions as described above.
    - The Client will coordinate all notification and instruction with the end user prior to the scheduled Reassignment date.
    - The Client will coordinate shipping of the re-assigned Endpoint device to its new assigned owner.
    - Ricoh will configure the re-assigned Endpoint for the new owner.
    - The Endpoint will be provisioned as a new Endpoint to the new owner via Autopilot as described above.

- **Endpoint retirement:**
    - The Client Representative may request permanent retirement of an Endpoint.

- This action is usually paired with provisioning a new endpoint to the end user.
- The Client will coordinate all notification and instruction with the end user prior to the scheduled Retirement date.
- Ricoh will reset the retired endpoint via Autopilot on a predetermined date/time.
- The Client will coordinate shipping of the retired Endpoint device to company offices for disposal.

Note: Any Endpoint administration workflow requirements beyond this scope are considered “custom”. Ricoh will apply a feed for custom Endpoint administration.

Mobile Endpoint Service Description for Ricoh Work Anywhere

Overview

What is Ricoh Work Anywhere Mobile Endpoint?

Ricoh Work Anywhere Mobile Endpoint services are designed to address the management of company-provided Office 365 apps and company-owned mobile devices provisioned to employees for business use:

- Standardized policy-driven deployment and management of Office 365 apps on personal and company mobile devices.
- Standardized policy-driven mobile device configuration, enrollment, access and compliance.
- Secured Office 365 apps and data management on mobile devices.
- Selective app wipe (personal devices) or full device wipe (company devices).
- Managed device inventory.

Ricoh Work Anywhere Windows Endpoint Service Tiers

There are two tiers of service for Ricoh Work Anywhere Mobile Endpoint:

Mobile Application Management (MAM)	Mobile Device Management (MDM)
Included in All RWA Bundles This level of service includes configuration, deployment, and support of company-provided Office 365 applications for business use on personal employee mobile devices. • Ricoh-managed policy-based app deployment and self-service enablement. Device enrollment not required. • Office 365 applications are configured to be containerized, encrypted, and secure on the mobile device. • Ricoh-managed data controls prevent storage of corporate data on the personal device, or redirecting data outside the Microsoft cloud ecosphere to employee personal cloud storage, etc. • Maintain complete separation between personal device features, settings, and business apps on the same device. • On-demand selective wipe of only the business applications on a personal device. Personal settings, content, etc. are not affected. Mobile Application Management is included in Ricoh Work Anywhere bundles and not sold as a separate add-on service.	**Included in Mobile Device Management Add-on option** This level of service includes all the features of MAM, plus management and support of company-owned devices provisioned to employees and approved users for business use. Ricoh manages: • Mobile device enrollment • Mobile device configuration • Mobile device conditional access and compliance • On-demand full mobile device wipe • Device inventory reports. Mobile Device Management **is not included** in Ricoh Work Anywhere bundles and is sold & provided as a **separate add-on service**.

Service Requirements

Ricoh Work Anywhere

MAM:

The client's end users must be enrolled in a Ricoh Work Anywhere service bundle that contains this service.

MDM:

The client's end users must be enrolled in a Ricoh Work Anywhere service bundle.

Microsoft Licensing

The end users utilizing these services must be licensed as per the appropriate Microsoft subscription requirements for Ricoh Work Anywhere services.

Services Enablement

MAM:

This service is included in Ricoh Work Anywhere bundles and not sold separately. Therefore, each user enrolled in a Ricoh Work Anywhere bundle is entitled to the service.

Client management may decide that some or all of the users should not have this service capability. So, while the service is included in the bundle, the client may elect to disable the capability for some or all end users.

MDM:

The client likely requires MDM capabilities for a subset of their workforce. Therefore, this service is sold as a separate add-on to Ricoh Work Anywhere bundles in the quantity the client requires (but cannot exceed the Ricoh Work Anywhere bundle quantity).

Mobile Endpoint Requirements

Mobile Endpoints must meet these Operating System requirements (MAM and MDM):

- OS types: Android an Apple iOS
- OS versions must be within the provider's defined active date range of supported Operating Systems
- OS must be configured to self-update with updates received from the OS provider and as per the OS provider schedule.
- OS type & version must be compatible with Microsoft Intune Endpoint Management capabilities. Refer to Microsoft documentation on mobile device compatibility with Intune.
- The Mobile Endpoint OS and device must conform to the manufacturer or cellular carrier/provider approved configuration and installed apps. Non-conforming devices (aka "jailbroken" devices) do not qualify for this service.

Mobile Endpoints must meet these device requirements (MDM only):

- Device must be purchased and provisioned to end users by the client company.
- Device must be from a Ricoh-recognized manufacturer.
- Device must be within the manufacturer's active lifecycle, and not considered to be End of Support (EoS) or End of Life (EoL) as defined by the manufacturer, or cellular service carrier/provider (if applicable).
- Device must be covered by a manufacturer or cellular service carrier/provider hardware warranty, or equivalent 3rd-party warranty.

- Device must be covered by a manufacturer or cellular service carrier/provider support plan, or equivalent 3rd-party support plan.
- Optional but preferred: Device Accidental Damage & Theft Protection service provided by the manufacturer, cellular carrier/provider, or equivalent 3rd-party protection.
- Device must include active endpoint protection app(s) provided by the device manufacturer or cellular carrier/provider.
- Device make & model must be compatible with Microsoft 365 use and Microsoft Intune Endpoint Management capabilities. Refer to Microsoft documentation on mobile device compatibility with Intune.

Ricoh Service Delivery

The device must be purchased through Ricoh to qualify for:

- Incident Support
- Hardware failure, damage, or theft replacement coordination as per warranty or protection plan

Ricoh's ability to troubleshoot device network and Internet connectivity issues depends on the type of network the device is connected to, and if that network is managed by Ricoh (or not). Ricoh has the greatest chance of resolving device connectivity issues when the device is connected to the company network that is also managed by Ricoh. Ricoh cannot troubleshoot:

- Devices connected to non-company networks
- Devices connected to company networks not managed by Ricoh
- Devices connected to the Internet via cellular service providers
- Devices connected to public networks

Service Responsibilities

■ (or Ricoh)	Ricoh responsibility	+	add-on service or capability
Client (or blank)	client responsibility	$	additional fee may apply (determined by Ricoh)
←	joint Ricoh / client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included

Any feature, function, service, or responsibility not expressly included or mentioned in this service description document is implied to be the client's responsibility.

Customer Success & Advisory Services

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description documentation for general service entitlements and availability.

In addition, these service entitlements apply for this service.

	Mobile Endpoint MAM (Included in all RWA Bundles)	Mobile Endpoint MDM (included in Mobile Device Management Add-on option)
Service Experience Analytics		
Microsoft Mobile Endpoint Inventory: Enrolled Device - Name - Manufacturer - Model - OS - OS Version - Primary User - Enrollment Date - Jailbroken Status		■

Proactive Incident Detection & Response

Ricoh does not provide distinctive Monitoring & Alerting for Microsoft 365 mobile device features and capabilities. Work Anywhere users are provided Microsoft's native capabilities for Monitoring data collection, Event identification, and Alerting for Microsoft 365 products.

Helpdesk & Support Services

Ricoh Helpdesk and Support services work with users to reactively troubleshoot and resolve incidents that occur through the normal usage of Ricoh-configured and supported features and functions.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, supported features for this service are shown in Appendix A of this document.

Solution Administration

Service solution administration is the day-to-day service activities surrounding individual users or devices engaged in using the service. These tasks typically do not require Ricoh Change Control review.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, these service entitlements apply.

	Mobile Endpoint MAM (Included in all RWA Bundles)	Mobile Endpoint MDM (included in Mobile Device Management Add-on option)
Mobile Endpoint Administration		
BYOD Mobile Endpoint self-service enrollment operations	n/a	n/a
Ad Hoc company Mobile Endpoint enrollment		■
Ad Hoc company Mobile Endpoint disable		■
Ad Hoc Mobile Endpoint company applications wipe	■	■
Ad Hoc company Mobile Endpoint device wipe / factory reset		■
Administration Request Processing		
Included Service Administration Requests *(per 50 users)*	5 per month	5 per month
Additional Service Administration Requests	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+

Solution Configuration Management

Service solution configuration changes affect many users or the entire client organization. Therefore configuration change requests require formal Ricoh Change Control review and approval before being implemented.

Approved changes can include planning, testing, and phased or scheduled releases by Ricoh engineers; therefore configuration changes may require additional fees to implement depending on the scope and complexity of the change.

Note: Ricoh reserves the right to deny solution configuration change requests that negatively impact the Ricoh-configured SSRC performance and security. Other solution change requests may lie outside the managed scope of the Ricoh-configured SSRC and may be rejected or qualify as scoped & planned engineering engagements. Additional fees may apply.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

In addition, these service entitlements apply.

	Mobile Endpoint MAM (Included in all RWA Bundles)	Mobile Endpoint MDM (included in Mobile Device Management Add-on option)
Mobile Endpoint Management		
Mobile Applications		
Intune Microsoft Office Mobile App Deployment Policy add/change/remove	■	■
Intune Mobile App Protection Policy add/change/remove	■	■
Mobile Endpoint Devices		
Intune Conditional Access Policy add/change/remove		■
Intune Android Enrollment & Restriction Policy add/change/remove		■
Intune Android Device Configuration Profile add/change/remove		■
Intune Android Device Compliance Policy add/change/remove		■
Intune Android Update Policy add/change/remove		
Intune iOS/iPadOS Enrollment & Restriction Policy add/change/remove		■
Intune iOS/iPadOS Configuration Policy add/change/remove		
Intune iOS/iPadOS Compliance Policy add/change/remove		
Intune iOS/iPadOS Update Policy add/change/remove		
Configuration Change Request Processing		
Included Configuration Change Requests *(per 50 users)*	3 per month	3 per month
Additional Configuration Change Requests	*(per request $)*	*(per request $)*
Bulk Request Processing	$+	$+

Mobile Endpoint Lifecycle Management

Lifecycle Management consists of activities regularly conducted to keep a system, device, or service current and up-to-date, or to make service course corrections based on changing technology requirements.

Lifecycle Management begins with an observed Lifecycle Event which is usually announced and scheduled in advance by a solution or service provider. Some are regularly scheduled repeat activities, others are one-time changes.

Lifecycle Events need to be assessed, tested, and approved before integrating with a managed service. Events may constitute minor or major changes to service architecture and incur costs to both Ricoh and the client.

Rich will endeavor to maintain foresight of upcoming Lifecycle Events and regularly-scheduled Events, and plan, validate, and test prior to general application to our service offerings.

Refer to the Ricoh Work Anywhere Bundles and Work Anywhere Essentials service description for general service entitlements and availability.

Note: Ricoh reserves the right to deny Lifecycle Events that negatively impact the Ricoh-configured SSRC performance and security. Other Events may lie outside the managed scope of the Ricoh-configured SSRC and may be rejected or qualify as scoped & planned engineering engagements.

	Mobile Endpoint MAM (Included in all RWA Bundles)	Mobile Endpoint MDM (included in Mobile Device Management Add-on option)
Mobile Endpoint Lifecycle Management		
Personal Endpoints		
New Mobile Endpoint apps deployment	End user self-service	■
Mobile Endpoint app updates	Manufacturer or Cellular Carrier/Provider	Manufacturer or Cellular Carrier/Provider
Company Endpoints		
New Mobile Endpoint deployment		■
Mobile Endpoint device OS updates		Manufacturer or Cellular Carrier/Provider
Mobile Endpoint device EOS/EOL tracking & replacement planning		
Mobile Endpoint device warranty/support expiration tracking		
Mobile Endpoint device warranty/support renewal coordination		
Mobile Endpoint device retirement		
Mobile Endpoint device ordering, shipping, & return coordination		
Configuration Change Request Processing		
Included Configuration Change Requests *(per 50 users)*		3 per month
Additional Configuration Change Requests		*(per request $)*
Bulk Request Processing		$+

Appendix A: Supported Service Features: Work Anywhere Windows Endpoint

The below list represents the **full** Microsoft 365 feature stack plus related Ricoh-provided solution features. Different components of Ricoh Work Anywhere will reference different portions of the list and will be reflected in each component's separate service description document.

The list below represents supported features for Ricoh Work Anywhere Windows Endpoint.

Note: features may change as per Microsoft discretion. Always refer to Microsoft's latest M365 feature definitions for the plans defined for Work Anywhere.

■ (or Ricoh)	Ricoh responsibility	$	additional fee may apply (determined by Ricoh)
Client (or blank)	client responsibility	$+	scoped professional services engagement
User	client user responsibility	n/a	not applicable / not included
+	add-on service or capability		

	OS Protect	Managed Endpoint
Microsoft 365 Application Support		
Microsoft Office 365 (Web)		
Microsoft Office 365 (Desktop)		
Microsoft Office 365 (Mobile)		
Visio for the Web		
Microsoft Loop components, pages, and workspaces		
Microsoft ClipChamp		
Microsoft Editor		
Multilingual Office Apps Interface		
Microsoft Office Shared Computer Activation		
Microsoft Exchange Online Support		
User, Resource, Inactive Mailboxes		
Distribution Lists & Contacts		
Calendars		
Public Folders & Mailboxes		
In-Place Archiving & Auto-Expanding Archive		
Microsoft Shifts		
Microsoft Bookings		
Microsoft Teams		
Teams Online Chat		
Teams Online Meetings		
Teams Live Events		
Teams Webinars (created & coordinated by customer employees)		
Teams Audio Conferencing		
Teams Avatars		
Teams Phone		
Teams File Sharing & Co-Authoring		
Microsoft SharePoint Online, OneDrive & Yammer		
Microsoft SharePoint Online Sites, Lists, Libraries		
Microsoft OneDrive & Known Folder Redirection		
Microsoft Viva Connections		
Microsoft Viva Engage		
Microsoft Yammer		
Microsoft 365 Knowledge, Insights, & Content		
Microsoft Graph API		
Microsoft Search		
Microsoft Stream		
Microsoft Forms		

Microsoft Lists		
Microsoft Delve		
Expertise identification		
Document Understanding/Form Processing		
Access Content Centers		
Document Understanding/Form Processing Metadata Viewing		
Microsoft Viva Insights		
Microsoft Viva Learning		
Microsoft 365 Analytics & Insights		
Microsoft Secure Score		
Microsoft Adoption Score		
Microsoft Compliance Score		
Microsoft Vulnerability Score		
Microsoft 365 Project & Task Management		
Microsoft Planner		
Microsoft To-Do		
Automation & App Development		
Microsoft Power Apps for Microsoft 365		
Microsoft Power Automate for Microsoft 365		
Microsoft CoPilot Studio for Teams		
Dataverse for Teams		
Microsoft 365 Copilot		
Microsoft Copilot (Edge Browser)		
Microsoft Copilot for Office Applications		
Microsoft Copilot for Teams		
Microsoft Copilot Studio		
Microsoft 365 Endpoint & App Management		
General		
Intune Endpoint Device Enrollment & Restriction policies	■	■
Intune Endpoint Device Conditional Access policies	■	■
Intune Endpoint Device Compliance policies	■	■
Intune Endpoint Windows Hello Policies		
Windows 10+ OS Endpoints		
Intune Windows Endpoint Configuration Profiles		
Intune Windows Endpoint Security Baselines		
Intune Update Rings (Ricoh standard configuration)		
Intune Update Rings (custom configuration)		
Intune Quality Updates for Windows 10+ Endpoint OS		
Intune Feature Upgrades for Windows 10+ Endpoint OS		
Windows 365 Cloud PC Endpoint		
Intune AutoPilot Profiles: Windows Endpoint (Ricoh standard configuration)		
Intune AutoPilot Profiles: Windows Endpoint (custom configuration)		
macOS Endpoints		
Intune macOS Enrollment Configuration	■	■
Intune macOS Endpoint Configuration Profiles		■
Intune macOS Compliance Policies		■
Intune macOS Endpoint Update Profiles		
Mobile Endpoints - Android		
Intune App Configuration policies: Mobile M365 Apps		
Intune App Protection policies: Mobile M365 Apps		
Intune Mobile Device Management polices		
Intune iOS provisioning profiles configuration		
Mobile Endpoints – iOS/iPadOS		
Intune App Configuration policies: Mobile M365 Apps		
Intune App Protection policies: Mobile M365 Apps		
Intune Mobile Device Management polices		
Intune iOS provisioning profiles configuration		
Applications		
Intune Company Portal	■	■

Intune App Configuration policies: Windows Endpoint Office Apps	■	■
Intune App Configuration policies: Windows Endpoint Ricoh Productivity Apps bundle		■
Intune App Configuration policies: Mobile Office Apps	■	■
Office Apps Cloud Policy		
Windows Endpoint Devices		
Company owned & provisioned endpoint devices: OS		
Company owned & provisioned devices: Hardware		
Personal devices		
Endpoint Domain Enrollment		
Endpoint peripheral devices, docking / charging equipment, external monitors, or other wired / wireless connected devices		
Endpoint Network & Internet connectivity		
Endpoint device OS malfunction		
Endpoint device hardware malfunction		
Endpoint device failed hardware replacement coordination		
Endpoint device proactive hardware replacement coordination		
Microsoft 365 Threat Protection		
Microsoft Defender for Business		
Microsoft Defender for Endpoint Plan 1		
Microsoft Defender for Endpoint Plan 2	n/a	n/a
Microsoft Defender for Office 365 Plan 1		
Microsoft Defender for Office 365 Plan 2	n/a	n/a
Microsoft Defender for Identity	n/a	n/a
Microsoft Defender Application Guard for Office 365	n/a	n/a
Microsoft Defender Application Guard for Edge		
Microsoft Defender Antimalware		
Microsoft Defender Firewall		
Microsoft Defender Exploit Guard		
Microsoft Defender Credential Guard		
Microsoft Defender for IoT	n/a	n/a
BitLocker		
BitLocker To Go		
Windows Information Protection		
Safe Documents	n/a	n/a
Ricoh Threat Protection		
Ricoh Endpoint Protection: Windows Endpoint standard anti-malware		
Ricoh Endpoint Protection: Managed Security *Windows 10 endpoint Managed Detection (MDR) & Response + 24x7 SOC*	+	+
Microsoft Cloud Access Security Broker (CASB)		
Microsoft Defender Cloud Apps	n/a	n/a
Microsoft Defender for Cloud App Discovery		
App Governance in Defender for Cloud Apps	n/a	n/a
Office 365 Cloud App Security	n/a	n/a
Microsoft 365 Identity & Access Management		
Azure Active Directory Domains		
Azure Active Directory Administrative Units		
Azure Active Directory User & Guest Accounts (standard)		
Azure Active Directory User & Guest Accounts (custom)		
Azure Active Directory Registered Device Accounts		
Azure Active Directory Azure AD Joined Device Accounts		
Hybrid Active Directory Joined Device Accounts		
Azure Active Directory Registered Applications		
Azure Active Directory Service Principals		
Azure Active Directory Managed Identities (System & User assigned)		
Azure Active Directory External Identities		
Azure Active Directory RBAC Roles & Administrators		
Azure Active Directory Security Groups		
Azure Active Directory Dynamic Groups		

Microsoft 365 Groups		
Azure Active Directory Identity Governance	n/a	n/a
Azure Active Directory Application Proxy		
Self Service Password Reset		
Multi Factor Authentication		
Conditional Access		
Risk Based Conditional Access/Identity Protection	n/a	n/a
Verifiable Credentials / Decentralized Identity	n/a	n/a
Privileged Identity Management	n/a	n/a
Access Reviews	n/a	n/a
Entitlement Management	n/a	n/a
DirectAccess		
Single Sign-On (SSO)		
Windows Hello for Business		
Microsoft Advanced Threat Analytics		
Microsoft 365 Information Protection		
Microsoft Information Protection Plan 1 settings & policies configuration		
Microsoft Information Protection Plan 2 settings & policies configuration	n/a	n/a
Manual, default, & mandatory sensitivity labels		
Automatic sensitivity labels	n/a	n/a
Manual sensitivity labels for Teams Meetings	n/a	n/a
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive	n/a	n/a
Sensitivity labels based on advanced classification (ML, EDM)	n/a	n/a
Sensitivity labeling for containers in Microsoft 365		
Data Loss Prevention (DLP) for emails and files		
Basic Office Message Encryption		
Advanced Office Message Encryption	n/a	n/a
Customer Key	n/a	n/a
Personal Data Encryption		
Windows Information Protection		
Microsoft 365 Data Lifecycle Management		
Manual retention labels		
Basic org-wide or location-wide retention policies		
Rules-based automatic retention policies	n/a	n/a
Machine Learning-based retention	n/a	n/a
Teams message retention policies	n/a	n/a
Records Management	n/a	n/a
Microsoft 365 eDiscovery & Auditing		
Content Search		
Standard eDiscovery including Hold and Export		
Litigation Hold		
Premium eDiscovery	n/a	n/a
Standard Audit		
Premium Audit	n/a	n/a
Microsoft 365 Insider Risk Management		
Insider Risk Management	n/a	n/a
Communication Compliance	n/a	n/a
Information Barriers	n/a	n/a
Customer Lockbox	n/a	n/a
Privileged Access Management	n/a	n/a
Microsoft Universal Print		
Universal Print configuration for UP-Ready printers Controlled in the M365 cloud		
Universal Print configuration for non UP-Ready printers Requires UP Connector app installed on local workstation or server		

Managed Adoption Service Description for Ricoh Work Anywhere

Overview

What is Ricoh Managed Adoption Service?

Ricoh offers multiple tiers of training and adoption services that provide various levels of management and functionality designed to meet the needs of most organizations. At the core of each of the tiers is a Ricoh Service Adoption Specialist (SAS). The SAS works collaboratively with business leaders to understand business specific goals/objectives, current technology profile, and their associated proficiency. Utilizing this information, the SAS will develop learning paths, create training schedules, and host a monthly meeting to provide campaign analysis and drive continued roadmap development/management.

- Learning Paths – Learning paths combine videos, assessments, and more into modules that are focused on specific technologies. These modules are designed to drive user adoption by increasing employee understanding of a specific technology thus boosting confidence in its usage, determining its best use case, and leveraging it to increase productivity.

- Training Schedules – Training schedules combine one or more learning paths into groupings which can be assigned to users, groups, departments, or even users who share common titles. These training schedules allow for defined training campaign start and end dates as well as user level reporting.

- Campaign Analysis – While providing training and adoption services is important, simply assigning content will not drive the necessary behavioral changes and thus improved business outcomes. To better drive these changes and outcomes at the end of each training campaign the SAS will review metrics and provide business leaders an analysis of the campaign. This analysis includes reports on the users who successfully completed the entire campaign, those that partially completed it, and those who didn't start it. When applicable the analysis will also include reports on assessments which may part of the learning paths.

- Roadmap Development/Management – With the ever-evolving landscape of both technologies available in the Office/Microsoft 365 platform and cyber threats. The SAS will work closely with business leaders to develop and manage a training and adoption roadmap. This roadmap will be a progressive plan designed to meet the business specific goals/objects, develop the knowledge to fully utilize the technologies available in the Office/Microsoft 365 platform, and to recognize the latest in cyber threats.

To complete the above tasks, the SAS will leverage up to four of the following components of the Ricoh Managed Adoption Service depending on the tier selected.

- Office/Microsoft 365 Training and Adoption – The focus of this core component is to empower employees with the knowledge they need to leverage the features of the Office/Microsoft 365 platform. This increases employee satisfaction, enables more effective hybrid work, boosts effective collaboration, and drives improved productivity.

- Security Awareness Training – The focus of this core component is to equip employees with the knowledge they need to protect themselves and their organization's assets from cyber threats. Every day, new cyber risks and unique data security challenges emerge. As these cyber threats continue to rise everyone in an organization plays an increasingly important role in recognizing, avoiding, and reporting cyber threats which may include phishing, spoofing, social engineering, and ransomware.

- Simulated Phishing Campaigns – While providing security awareness training is essential, testing an employee's response to an event is the only way to ascertain their true understanding of the concepts. The simulated phishing campaign enable employers to validate their employee's ability to recognize cyber threats and provide remedial training as necessary.

- Custom Content Publishing – Leveraging custom content business can utilize the Ricoh Managed Adoption Service as a Learning Management System (LMS) for all aspects of their business. This increases the platforms functionality by

allowing business to have Ricoh publish custom content (videos, PDFs, Office documents, and graded/ungraded assessments), develop learning paths, and create training schedules for any topic. Use case examples include employee onboarding, internal systems training, open enrollment/benefits enrollment, etc.

Ricoh Managed Adoption Services Components and Tiers

The service components are combined into the service tiers outlined below.

Service Components	Basic (Included in RWA)	Standard (Included in RWA Safe)	Advanced (Included in RWA Safe Plus)
Service Adoption Specialist	X	X	X
Learning Management Platform	X	X	X
Office/Microsoft 365 Training and Adoption	X	X	X
Security Awareness Training	X	X	X
Simulated Phishing Campaigns		X	X
Custom Content Publishing			X

Service Prerequisites

The Ricoh Managed Adoption Service is designed to enhance employee engagement and productivity as it relates to the Microsoft 365 service stack. Therefore, requiring the following prerequisites be met.

- Customer enrollment in Ricoh Work Anywhere Service
- Customer purchases and maintains a quantity of 50 or more Ricoh Managed Adoption Service seats.
  - **AND**
- Customer purchases and maintains a corresponding quantity of
  - Ricoh provided Microsoft 365 Business Premium/E3/F3 licenses
  - **AND**
  - Ricoh provided Microsoft 365 Business Premium/E3/F3 Essentials Support Bundles

Details of the prerequisite Ricoh managed services are not governed herein.

Technical Requirements

Employees who require access to Ricoh Managed Adoption Service must maintain an active Office/Microsoft 365 license.

Services Summary

Services Summary
Implementation
Services to configure and implement the Ricoh Managed Adoption Service are provided as part of a separate time & materials engagement. Therefore, the implementation services are outside the scope of these services.
Management Summary
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.

Roles and Responsibilities

Description	Basic (Included in RWA)	Standard (Included in RWA Safe)	Advanced (Included in RWA Safe Plus)
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 • Provide training campaign analysis			Ricoh
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

Backup for Microsoft365 Service Description for Ricoh Work Anywhere

Overview

What is Backup for Microsoft 365?

Microsoft 365 is the predominant remote / in-office / hybrid workforce service solution in use today and continues to accelerate in growth and popularity for companies of all sizes, in all markets.

Service Solution Summary

Ricoh Backup for Microsoft 365 is a Ricoh-managed, cloud-based proactive data protection backup solution for key Microsoft 365 cloud-based data, files, and email.

Enrollment Conditions & Dependencies

Minimum enrollment requirements:
The customer's user, guest, and temporary accounts must be enrolled in one of the following:

- Microsoft Office 365 Enterprise subscription (including or not including Microsoft Teams)
- Microsoft 365 Business or Enterprise subscription (including or not including Microsoft Teams)
- Microsoft Teams Enterprise add-on to Microsoft or Office 365 subscriptions that do not include Microsoft Teams
- Ricoh Work Anywhere services and adhere to the enrollment conditions thereof
- Ricoh Managed Microsoft 365 services and adhere to the enrollment conditions thereof

Microsoft dependencies:
The Ricoh services described in this document are contingent upon Microsoft 365 features and capabilities as determined and provided by Microsoft. Microsoft may, at times, add, change, or remove features and capabilities that impact this service's ability to function as planned. Ricoh and our associated service solution provider(s) will work to maintain currency and relevancy with Microsoft changes as they occur to preserve service continuity for our customers. This may result in changes to this service solution capabilities and Ricoh's management of the solution for the customer.

Service solution dependencies:
The Ricoh services described in this document are contingent upon the service solution provider(s) features and capabilities as determined by the solution provider(s). These features and capabilities are defined by the solution provider(s) and may change over time. Ricoh will work with our service solution provider(s) and customers to ensure successful solution operation and continuity. This may result in changes to this service solution capabilities and Ricoh's management of the solution for the customer.

Subscription & Licensing Requirements

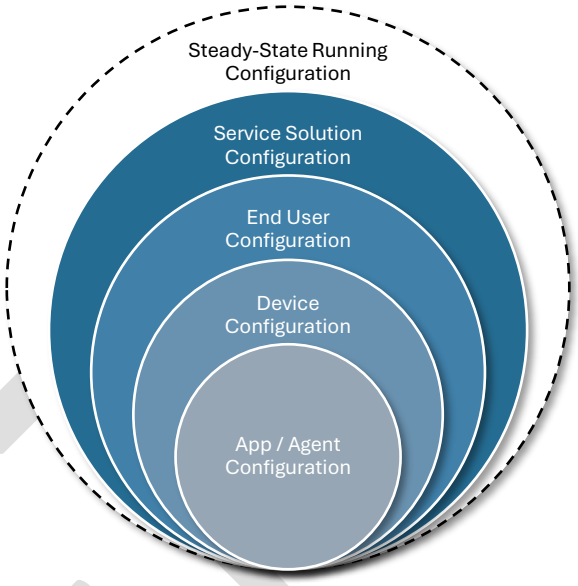
- Ricoh Backup for Microsoft 365 requires a service account with Global Administrator Role Based Access Control (RBAC) permissions in the customer's Microsoft 365 tenant.
- Ricoh Backup for Microsoft 365 may require the service account to be licensed with an appropriate Microsoft 365 core license in order to realize the full extent of backup capabilities. In this event, the service account will be licensed accordingly, and the license cost will be billed to the customer separately from the service fees associated with this service offering.
- Ricoh Backup for Microsoft 365 service fees include the requisite solution licensing required to facilitate the solution's functionality as described herein.

Supported Service Solution Features

See **Appendix A** in this Service Description

Service Implementation

1. Ricoh's service offering implementation & onboarding is conducted as a standardized Professional Services engagement defined by a Scope of Work (SOW) that enables a Best Practice implementation of Ricoh services.
2. **Service Solution Configuration:** Ricoh's supported implementation will configure all requisite solution subscriptions, features and capabilities as per Ricoh's standardized Best Practice deployment model in accordance with this service description.
   - Solution configuration includes creation of service accounts with admin privileges in the customer's Microsoft tenant.
   - Solution configuration testing may be conducted prior to enabling the solution for general use.



3. **End User Onboarding:** Ricoh Backup for Microsoft 365 is configured for each user account in the Microsoft 365 cloud configuration. User interruption / interaction is not necessary.
4. **Device Onboarding:** Ricoh Backup for Microsoft 365 does not require device configuration or onboarding.
5. **Applications & Agents:** Ricoh Backup for Microsoft 365 does not require applications or agents to be installed on end user devices.
6. **Steady-State Running Configuration (SSRC):** Is defined as the entirety of the service solution configuration, end user configuration, device configuration, and applications/agents installed and configured for the service. Ricoh is responsible for the SSRC solution configuration, administration, and change management of the solution as configured by Ricoh.

Changes to any part of the SSRC made are subject to Ricoh Change Management Governance (see Service Definitions & Conditions).

Service Tiers

Ricoh Backup for Microsoft 365 is offered in one tier of service.

- ■ Ricoh service responsibility
- ▲ Joint Ricoh/Customer responsibility
- ★ Defined through adjacent / parent Ricoh service dependency (noted in Enrollment Conditions & Dependencies)
- \+ Add-on service or capability
- $ Additional fee may apply (pending Ricoh review)
- n/a Not Available

Customer Success & Advisory Services

Ricoh does not assign a Customer Success Manager or Technology Consultant to the customer for this service.

The following Customer Success actions will be provided with Ricoh Backup for Microsoft 365 services.

Customer Success & Adoption Management		Operations Owner
Service Experience Analytics		Service Delivery
Automated Scheduled Backup Success / Fail Reporting	Weekly (email)	Data Protection Specialist

Reactive Service Incidents

Ricoh's Helpdesk & Support services are designed to help users resolve problems that occur through the usage of Ricoh-configured service solution features and functions (See Appendix A).

Reactive Incident Management		Operations Owner
Support Incident Availability		
Helpdesk Hours of Operation –Support Incident Submission *Eastern Standard Time (EST)*	7am-7pm (M-F) Remote POC Only	CCare
Support Incident Contact Options	Ricoh Portal Telephone Email Chat	CCare
Reactive Incident first response	Ricoh	CCare
Reactive Incident escalation to Ricoh Specialist	Ricoh	Data Protection Specialist
Reactive Incident escalation to Microsoft troubleshooting & resolution	Ricoh	Data Protection Specialist
Reactive Incident escalation to 3rd Party provider troubleshooting & resolution	Ricoh	Data Protection Specialist
Backup-Related Incident Types		
Incidents created by proactive backup success/fail monitoring & reporting	■	Data Protection Specialist

Proactive Service Detection & Response

Proactive service monitoring, event detection, alert generation, and notification is provided by Ricoh, the primary solution provider, and 3rd party providers. This section outlines the frameworks, resources, and responsibilities for Ricoh and solution providers associated with this service offering.

Proactive Detection & Response		Operations Owner
Event Detection		
Primary Solution Provider (provider terms and conditions apply)		
Planned Maintenance Events	■	Provider
Unplanned Downtime Events	■	Provider
Service Degradation	■	Provider
Service Health Status	n/a	
Ricoh		
Planned Maintenance Events	Provider notification	Data Protection Specialist
Unplanned Downtime Events	Provider notification	Data Protection Specialist
Service Degradation	Provider notification	Data Protection Specialist
Service Health Status	Backup Success/Fail Review Once per day (Monday-Friday) • Two or more consecutive backup failures • Consistent periodic backup failures	Data Protection Specialist
Alert Generation		
Primary Solution Provider (provider terms and conditions apply)	Backup Success/Fail Reporting	Data Protection Specialist
Alert Notification		
Primary Solution Provider (provider terms and conditions apply)		
Primary Notification method	Provider Management Portal	Provider
Ricoh		
Primary notification method	Customer POC email notification (manual)	Data Protection Specialist
Event Response		
Ricoh Incident creation	Ricoh	Data Protection Specialist

Service Administration

Administration is the day-to-day service activities surrounding individual users or devices engaged in using the service. These tasks typically do not require Change Control review but must be initiated by an authorized customer POC.

Service Administration		Operations Owner
Service Request Availability		
Hours of Operation – Administrative Request submission *Eastern Standard Time (EST)*	7am-7pm (M-F) Remote	CCare
Administrative Service Request contact options	Ricoh Portal Telephone Email	CCare
Data Backup		
Service Request Submission	POC Only	
On-Demand backup (outside of normal schedule)	■	Data Protection Specialist
Data Restore		
Service Request Submission	POC, End Users	
Restore Destination: In-Place	■	
Restore Destination: Non-Destructive	$ Scoped Professional Service engagement required	Professional Services Data Protection Specialist
Restore Request quantity: Included in service	Up to 5 per month	
Restore Request quantity: Additional	$ Per-request fee applies	

Level 1 Restore:
• Up to (5) users per request:
  ○ Select OneDrive Cloud Files & Folders
  ○ Exchange Online Emails, Calendar, Contacts, Tasks, Full Mailbox
• Company:
  ○ Select SharePoint Files & Folders
• Validation & Triage:
  ○ Determine data to be restored.
  ○ Attempt restore via native Microsoft systems and methods (examples: previous versions, undelete files/email, etc.)
  ○ Restore from Backup if necessary
	■	CCare Tier 2

Level 2 Restore:
• Above (5) users per request:
  ○ Select OneDrive Cloud Files & Folders
  ○ Exchange Online Emails, Calendar, Contacts, Tasks, Full Mailbox
• Company:
  ○ Exchange Online Public Folders
  ○ SharePoint Sites, Lists, Libraries, Collections
  ○ Microsoft Teams content
	■	Data Protection Specialist

Level 3 Restore: • Non-standard restore operations that require additional engineering, resources, time and materials, etc. beyond restoring actual data from backup.	$ Scoped Professional Service engagement required	Professional Services Data Protection Specialist
Test Restore: Periodic test of restore operations efficacy	$ Scoped Professional Service engagement required	Professional Services Data Protection Specialist
Backup Export		
Service Request Submission	POC Only	
On-Demand backup data export	$ Per-request fee applies	Data Protection Specialist

General		
Service Request Submission	POC Only	
User account add/change/remove – POC only request	■	Data Protection Specialist
Inactive account backup pause – POC only request	■	Data Protection Specialist
Inactive account data deletion – POC only request	■	Data Protection Specialist

Solution Configuration Change Management

Aspects of the service solution configuration can potentially impact all users & devices in a customer's organization. These changes need to be reviewed and approved through a formal Change Control process; and undergo planned and tested general release processes.

Service Configuration Management is performed by Ricoh and in some cases, may incur additional fees depending on the nature and extent of the change.

Solution Configuration Change Management		Operations Owner
Service Request Availability		
Hours of Operation – POC Service Management Request Submission *Eastern Standard Time (EST)*	7am-7pm (M-F) Remote	CCare
Administrative Service Request Contact Options	Ricoh Portal Email	CCare
Company Organizational Bulk Changes		
Company Acquisition / Merge / De-Merge *(requires requisite notification and lead time to review, plan, and execute)*	$ Scoped Professional Service engagement required	Customer Success
Bulk Organizational Changes *(large-scale changes to personnel, departmental changes, facility expansion/reduction)* *(requires requisite notification and lead time to review, plan, and execute)*	$ Scoped Professional Service engagement required	Customer Success
Service Termination		
Upon termination of service, accumulated customer backup data can be retained for a monthly fee, and restored via request. The backup data will expire on schedule until all restore points are expired. Alternatively, the customer may request a full deletion of backup data upon termination.		
Post-termination data retention	$ Monthly retention fees	Data Protection Specialist
Post-termination data deletion - Scheduled deletion of data at expiration	■	Data Protection Specialist
Post-termination data deletion – On-Demand deletion of data (written & acknowledged verification required)	■	Data Protection Specialist
Post-Termination on-demand backup data export	$ Scoped Professional Service engagement required	Data Protection Specialist
Post-termination restore from backup requests	$ Per-request fee applies	Data Protection Specialist

Service Lifecycle Management

Ricoh ensures that the service remains relevant and in-step with changes made by the service solution provider(s), as well as changes made by Ricoh to improve service delivery and value realization over time.
Ricoh conducts quarterly review of the service KPIs and upcoming solution provider changes, and maintains a service improvement roadmap to review, approve, plan, and implement required changes with minimal to no impact to customers and end users.

Service Lifecycle Management		Operations Owner
Service Change Event Management		
Service Lifecycle Change Event Generation	Ricoh / Solution provider	Service Owner
Service Lifecycle Change Event Assessment, Planning, Testing, & Implementation	Ricoh	Service Owner Data Protection Specialist
Service KPI Measurement & Analysis (internal)		

Service Enrollment audit & review	Quarterly	Service Owner
Service Health audit & review	Quarterly	Service Owner
Service Incident / Request audit & review	Quarterly	Service Owner
Lifecycle Management		
Solution provider application updates	Solution provider	Solution provider

Appendix A: Service Solution Features

The following is a list of solution features and capabilities associated with the Backup for Microsoft 365 service offering. The features listed are subject to change by the solution provider at any time.

Backup for Microsoft 365 Solution Features	
Backup Content	
The customer is responsible for the actual data content being backed up by this service. The conditions of the content must meet the requirements of the backup service to ensure successful backup completion and data restore efficacy.	
OneDrive Cloud content	Cloud-based OneDrive content (Files, Sites, Lists) (includes permissions & metadata)
Exchange Online content	Personal & Shared Mailboxes, Contacts, Calendars, Public Folders, Tasks, Notes
SharePoint Online content	Company files and folders (Sites, Collections, Sub-Sites, Documents, Libraries) (includes permissions & metadata)
Microsoft Teams content	Sites, Channels, Calendars (includes permissions & metadata)
User Device content	**User device data is not included in backup** Local content synchronized to OneDrive cloud is backed up via OneDrive Cloud (see above)
Source Content Changes	
Automatic new user/site source activations (manual operation not required)	New user OneDrive space New user mailbox/contacts/calendars New Public Folders New SharePoint content New Teams content
Deleted source content (deleted from original source)	Maintained in backup storage until retention expiration
Backup Retention	
Backups require time to capture all the changes made to data. This is called the backup duration. The backup duration is impacted by the amount of data being backed up at any given time. In some instances, there is too much data to backup in the service's defined timeframe objective. When this happens, data backup will fail and restore points will be incomplete. Ricoh will work with the customer to identify problematic backup conditions that necessitate a backup frequency that is best to establish consistently successful and reliable backups for the customer. This frequency may differ from the service description's stated backup frequency targets.	
Backup Frequency (Restore Point) targets	Up to 3 times per day (every 8 hours) 365 days per year (up to 1,095 restore points)
Backup Restore Point Retention Period	1 Year
Backup Capacity	Unlimited
Backup Repository Storage Platform	Solution Provider's platform

Restore	
Restore Level: OneDrive cloud	All hierarchal levels From any captured restore point Includes metadata & permissions
Restore Level: Exchange Online	All hierarchal levels From any captured restore point Includes metadata & permissions
Restore Level: SharePoint Online	All hierarchal levels From any captured restore point Includes metadata & permissions
Restore Level: Microsoft Teams	All hierarchal levels From any captured restore point Includes metadata & permissions
Permissions-only restore (security rollback)	■
Metadata-only restore	
Restore to original source (aka in-place)	■
Restore to alternate location (aka non-destructive)	■