

Exhibit A: Service Brief for Ricoh Work Anywhere

Unauthorized Use Prohibited1

Overview2

Microsoft 365.....4

Other Service Solution Components.....4

Ricoh Work Anywhere Service Bundles5

Service Enrollment Conditions9

Add-On Services10

Services Implementation & Onboarding.....12

Glossary of Definitions14

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.

Overview

What is Ricoh Work Anywhere?

Ricoh Work Anywhere is designed for the needs of the modern hybrid workforce:

- Work from anywhere (office, home, travel)
- Work at any time (flexible works schedules)
- Work on a variety of endpoints (workstation, tablet, and phone)
- Work securely (protect identity, device, apps and data)
- Work productively (collaborate & communicate effectively with colleagues, and enhance the hybrid work experience)

Ricoh Work Anywhere provides a cloud-first hybrid work solution that is configured, supported, and managed by Ricoh:

- Cloud-based hybrid work solution that incorporates identity management, email, popular work applications, file data storage, and real-time communication & collaborative hub capabilities.
- Always-on accessibility from workstation, mobile endpoints, and the web.
- Managed backup of cloud-based data, email, and collaborative data.
- Managed adoption learning platform.
- Managed security for worker identities, workstation and mobile endpoints, data, applications, and malicious website protection; based on Zero-Trust security principles and the CIS framework.
- Managed security awareness training and phishing simulation.

Ricoh Work Anywhere is delivered, supported, and managed by Ricoh's hybrid work experts:

- Expert Best Practice solution design & configuration.
- Expert solution implementation and device / user onboarding.
- Expert service delivery performed by experienced professionals using enterprise-grade systems and solutions.
- Dedication to client success and technology growth through advisory and roadmap planning engagements.

Microsoft 365

Ricoh Work Anywhere is built on the core solution capabilities of **Microsoft 365 Business Premium**:








Cloud-First	Cloud-based SaaS solutions accessible through simple Internet connections
Identity Management	Microsoft Entra ID (formerly Azure Active Directory) identity and access management that includes Multi Factor Authentication + Conditional Access
Office Applications	Microsoft 365 Office applications (desktop, mobile, and web versions)
Email	Microsoft Exchange Online Email + Exchange Online Protection
Cloud Data	Microsoft One Drive personal cloud file & data storage
Collaboration	Microsoft Teams real-time collaboration & communications experience
Managed Apps & Devices	Intune unified workstation & mobile endpoint and application management
Automation & Self-Service	Self-service password reset Autopilot out-of-box self-service Windows workstation setup
Frontline Protection	Managed web access to data and apps Defender for Office 365 advanced Email & Teams protection

Other Service Solution Components

To ensure a best-in-class experience, Ricoh Work Anywhere services may utilize technology solutions developed by 3rd-party solution providers other than Ricoh or Microsoft. In many cases, the licensing for such solutions are included in the Ricoh Work Anywhere service fees and do not need to be purchased separately. Ricoh may change solutions and providers at Ricoh's sole discretion at any time. Such changes may necessitate changes to solution features and services capabilities. Ricoh will endeavor to provide the client with notice of changes in advance of implementation and to minimize disruption to the client.

Ricoh Work Anywhere Service Bundles

Ricoh Work Anywhere services are a combination of managed service solutions and capabilities:

	Managed Service	Description
	Ricoh Work Anywhere Essentials	Configuration, user support, and management of Microsoft 365 identity management, security, email, apps, data storage, collaboration and communication platforms.
	Windows Endpoint	Windows 10 /11 OS & workstation endpoint security, support, automated deployment and management.
	Mobile Application Management (MAM)	Managed Office mobile applications securely deployed and managed on personal devices.
	Microsoft 365 Backup	Managed backup & restore of Microsoft 365 Exchange Online email, One Drive data, SharePoint data, and Teams data.
	Managed Adoption Services	Managed learning platform with prescriptive learning paths for Microsoft 365, Security Awareness Training, email Phishing Simulation, and customized learning content.
	Managed Security	Advanced endpoint Managed Detection & Response (MDR) with 24x7 Security Operations Center (SOC)
	Managed Web Filtering	Managed defense against malicious websites and Dark Web monitoring.

Ricoh Work Anywhere 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 services and onboarding of users and endpoints 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.

To reduce complexity and offer clients the best prescriptive combination of services to achieve their desired outcomes, Ricoh Work Anywhere services are provided in curated **Bundles**.

Each Ricoh Work Anywhere bundle is designed to deliver value through combinations of solutions and levels of service. This allows clients to choose the right bundle to suit their business needs and grow and expand to higher levels of service over time.

Bundle	Company Type	Purpose
Ricoh Work Anywhere Small Business	Small Business (less than 50 users)	<ul style="list-style-type: none"> • Budget-minded small businesses that accept a shared operations services model at a lower price point. • Easy entry point for small businesses seeking hybrid work services. • Small businesses that seek to improve their cyber security posture.
Ricoh Work Anywhere	Small to Midsize Business (more than 50 users)	<ul style="list-style-type: none"> • Businesses that require basic hybrid work capabilities and security. • Businesses seeking provider-operated solutions and services. • Easy hybrid work entry point for budget-minded businesses.
Ricoh Work Anywhere Safe	Midsize to Large Business	<ul style="list-style-type: none"> • Businesses that seek robust hybrid work solutions and services. • Businesses seeking to partner with hybrid work experts for guidance, implementation, and ongoing service & solution operations. • Businesses that seek a strong cyber security baseline and reactive capabilities.
Ricoh Work Anywhere Safe Plus	Midsize to Large Business	<ul style="list-style-type: none"> • Businesses that seek maximum hybrid work solutions and services value. • Businesses that require the highest level of value realization and measurable success outcomes of hybrid work adoption.

The table below shows a summary of the included solutions and levels of service for each bundle.

			Work Anywhere Bundles			
			Ricoh Work Anywhere Small Business	Ricoh Work Anywhere	Ricoh Work Anywhere Safe	Ricoh Work Anywhere Safe Plus
Ricoh Work Anywhere Essentials	Basic	Ricoh-Configured Hybrid Work Solution: <ul style="list-style-type: none"> Ricoh-configured Best Practice Microsoft 365 solution <ul style="list-style-type: none"> Identity & Access management Zero-Trust Security Baseline Office365 desktop & web applications Always-on cloud-based email Always-on cloud-based file & data storage Teams: Cloud-based communications & collaboration Microsoft 365 subscription management Client-provided user account administration Annual service review engagements Annual Secure Score review & update Ricoh solution configuration management Microsoft 365 lifecycle management 	•			
	Advanced	Basic plus: <ul style="list-style-type: none"> Designated Client Success Manager Designated Technology Advisor Ricoh-provided user account & solution administration Quarterly service review engagements Annual executive business review engagement Semiannual Secure Score review & update Semiannual Utilization & Adoption Score review 		•	•	
	Premium	Advanced plus: <ul style="list-style-type: none"> Monthly service review engagements Semiannual executive business review engagement Quarterly Secure Score review & update Quarterly Utilization & Adoption Score review Quarterly Microsoft 365 Vulnerability review 				•
	User Helpdesk & Support Services					
		Helpdesk Availability	7am – 7pm M-F (remote)			
		Support Incident Submission	Client Rep. only	Client Rep. Users	Client Rep. Users	Client Rep. Users
		Support Incident Contact Options	Ricoh Portal Telephone Email Chat			
		Incident first response, troubleshooting, & resolution	Client	Ricoh	Ricoh	Ricoh
		Incident Escalation to Ricoh Solution Specialists	•	•	•	•
		Incident Escalation to 3 rd -Party Solution Providers	•	•	•	•
Managed Windows Endpoint	OS Protect	Windows 10 & 11 Operating System Management <ul style="list-style-type: none"> Ricoh-configured Windows OS settings Ricoh-provided OS Support Ricoh Standard Endpoint Anti-Malware protection Monthly OS Quality Updates Annual OS Version Upgrades Entitlement: One OS per enrolled user 	•			
	Windows Device	OS Protect plus: <ul style="list-style-type: none"> Ricoh-provided Best Practice workstation configuration Ricoh-configured Zero-Trust workstation security baseline Ricoh-provided Workstation Support Standard Microsoft Autopilot workstation deploy/reset Device inventory & Mfgr. support / warranty tracking Entitlement: One device per enrolled user 		•	•	•
Managed Mobile Applications	Mobile App Management (MAM)	Managed Business Apps on Personal Devices <ul style="list-style-type: none"> Suitable for corporate or personal mobile devices Mobile Application Management for Office365 mobile applications Mobile Application Security for Office365 mobile applications Mobile Application wipe / reset 	•	•	•	•

			RicoH Work Anywhere Bundles			
			RicoH Work Anywhere Small Business	RicoH Work Anywhere	RicoH Work Anywhere Safe	RicoH Work Anywhere Safe Plus
Data Protection	Microsoft 365 Backup	Managed Microsoft 365 Backup & Restore Managed backup & restore of Microsoft 365 Email, OneDrive, SharePoint, and Teams	•	•	•	•
Managed Adoption Services	Basic	Managed Microsoft 365 + Security Awareness Learning <ul style="list-style-type: none"> Managed Microsoft 365 Learning Platform Managed Security Awareness Training Structured Learning Paths Activity / Progress tracking & reporting 		•		
	Standard	Basic Plus: <ul style="list-style-type: none"> Managed Email Phishing Simulations Simulation results tracking & reporting 			•	
	Advanced	Standard Plus: <ul style="list-style-type: none"> Stage customized learning content Customized Learning Paths 				•
Managed Security Services	Standard	Managed Detection & Response (MDR): <ul style="list-style-type: none"> Advanced Windows Endpoint Security 24x7 Security Operations Center (SOC) Managed endpoint security incident isolation & remediation Escalate problems to Ricoh Specialists 	•		•	•
Managed Web Filtering	Basic	Office Location Protection <ul style="list-style-type: none"> Managed protection against malicious URLs and websites per office location Dark Web Monitoring 				
	Standard	Basic Plus: <ul style="list-style-type: none"> Managed protection for endpoints 			•	
	Premium	Standard Plus: <ul style="list-style-type: none"> Custom Web Content Filtering 				•

Note: Other conditions apply. See the Service Descriptions for each of the services included in the bundle for more detail.

Service Enrollment Conditions

Enrollment in Ricoh Work Anywhere services require the following:

- Ricoh Work Anywhere bundles are purchased as a package of services that cannot be purchased separately.
- All users utilizing Ricoh Work Anywhere services must be enrolled in the same services bundle. Clients cannot mix bundle choices for different segments of their workforce.
- Ricoh Work Anywhere bundles are designed and implemented with standardized features and configurations to ensure the security, consistency and quality of the service for our clients. Ricoh-selected elements of the bundle can be configured to client specification, but otherwise the standard solution configuration developed by Ricoh is the “steady-state running configuration” of the service.
- Endpoints:
 - Workstation Endpoints that run an Operating System (OS) other than Microsoft Windows can be registered into Microsoft 365 but are not subject to Managed Windows Endpoint Services.
 - Company Endpoints running a Windows OS utilized directly or shared by Ricoh Work Anywhere enrolled end users must be joined to Azure Active Directory (aka Microsoft Entra ID).
 - Ricoh Work Anywhere Microsoft 365 services are configured for secured availability via the Web from company and personal endpoints, provided the company provides authorization to end users.
 - Personal Mobile Endpoints may be utilized for Mobile Application Management services and do not require enrollment in Azure Active Directory.
- Ricoh does not support unauthorized client-initiated changes or 3rd-party changes made to the service’s Steady-State Running Configuration (SSRC) as implemented and managed by Ricoh. Other than where stated in this document and specific Service Descriptions, unauthorized changes made to the SSRC by the client or any 3rd party may invalidate the integrity of the SSRC and relieve Ricoh’s service responsibilities thereto.

All client or 3rd-party changes to the SSRC must be submitted to Ricoh as described above as Management Service Requests.

- Ricoh requires administrative-level access to workstations via Ricoh-configured Local Administrator accounts. Ricoh account credentials are reserved for Ricoh’s knowledge and use only.
- The service may include tools and utilities installed and upgraded by Ricoh on enrolled endpoint devices for the purpose of monitoring, reporting, and facilitating service delivery. Ricoh may choose to change or discontinue use of these applications at any time. Client refusal or other conditions that prevent these application installations and upgrades may result in relieving Ricoh of service responsibilities for the affected device(s).
- Ricoh Work Anywhere services include Ricoh administrative access to the Windows Desktop via local administrator accounts created exclusively for Ricoh use. Ricoh administrator account credentials are reserved for Ricoh’s knowledge and use only.

Note: Other conditions apply. See the Service Descriptions for each of the services included in the bundle for more detail.

Add-On Services

Ricoh Work Anywhere includes various add-on services that augment the value of the primary service bundles:

Mobile Device Management: Ricoh management of company-owned mobile devices and applications.

- Ricoh provided support and escalation to hardware manufacturer.
- Configure device conditional access policies, compliance policies, enrollment and restriction policies to protect devices from unauthorized access.
- Configure, deploy, and retire company-issued mobile phones, tablets, and Office mobile applications.
- Protection in case of loss or theft by disabling and wiping mobile devices and Office mobile apps.
- Device inventory & compliance checks.

Desktop Anywhere: Ricoh provisioned and managed cloud-based hardware-free Windows desktop experience that allows users to access their desktop from any device, at any time.

- Powered by Microsoft Windows 365 cloud PC technology.
 - Requires Microsoft Windows 365 licensing.
- Ideal for temporary and contract workers who utilize their own personal workstation endpoint (BYOD) devices.
- Provide a quality Windows desktop experience for any user on light-duty inexpensive workstation endpoint devices that only require an Internet connection.
- Quick & automated deployment (usually under one hour) utilizing Autopilot and Intune capabilities.
- Reset and Restore from Backup capabilities.
- Ricoh-provided standard or advanced endpoint protection options.
- Includes Windows OS Protect support and management.

Add-on services cannot be ordered as standalone services. Add-on services are available for clients that enroll in Ricoh Work Anywhere services. The client can order add-on services in any quantity that does not exceed the Ricoh Work Anywhere enrolled bundle quantity.

Note: Other conditions apply. Please refer to each add-on's service description documentation for more detail.

Services Implementation & Onboarding

Services implementation & onboarding is conducted as a Professional Services engagement defined by a standardized Scope of Work (SOW) that enables a Best Practice implementation of Ricoh Work Anywhere services.

Ricoh's supported implementation will configure the required subscriptions, features and capabilities as per Ricoh's standardized, Best Practice deployment model.

Ricoh will configure application policies for a Ricoh-defined suite of common productivity applications, web browsers, etc.

- This is called the **Ricoh Productivity Apps Bundle**. Ricoh is responsible for the configuration and management of these applications & settings.

Ricoh will enroll users into Ricoh Work Anywhere services. Users will be provided a "Welcome Packet" of information that includes informational content of the service, and instructional content for self-service MFA registration, self-service password reset, etc.

Ricoh will enroll Windows PC devices into the Microsoft 365 solution as **Azure AD joined** devices. This process involves a slight disruption of user workflow as the device is transitioned. This disruption comes in the form of one or more restarts of the workstation and logons to complete the transition process.

Ricoh will configure, implement, and onboard users and devices into the selected Ricoh Work Anywhere add-on services chosen by the client.

The implemented Ricoh Work Anywhere bundled solutions and services, as well as the onboarded end users & devices, constitutes the **Steady-State Running Configuration (SSRC)** of the service solutions.

Note: Ricoh is responsible for the overall SSRC solution configuration.

The SSRC includes features and configurations that affect the entire client organization, individual users, and endpoint devices such as workstations and mobile devices.

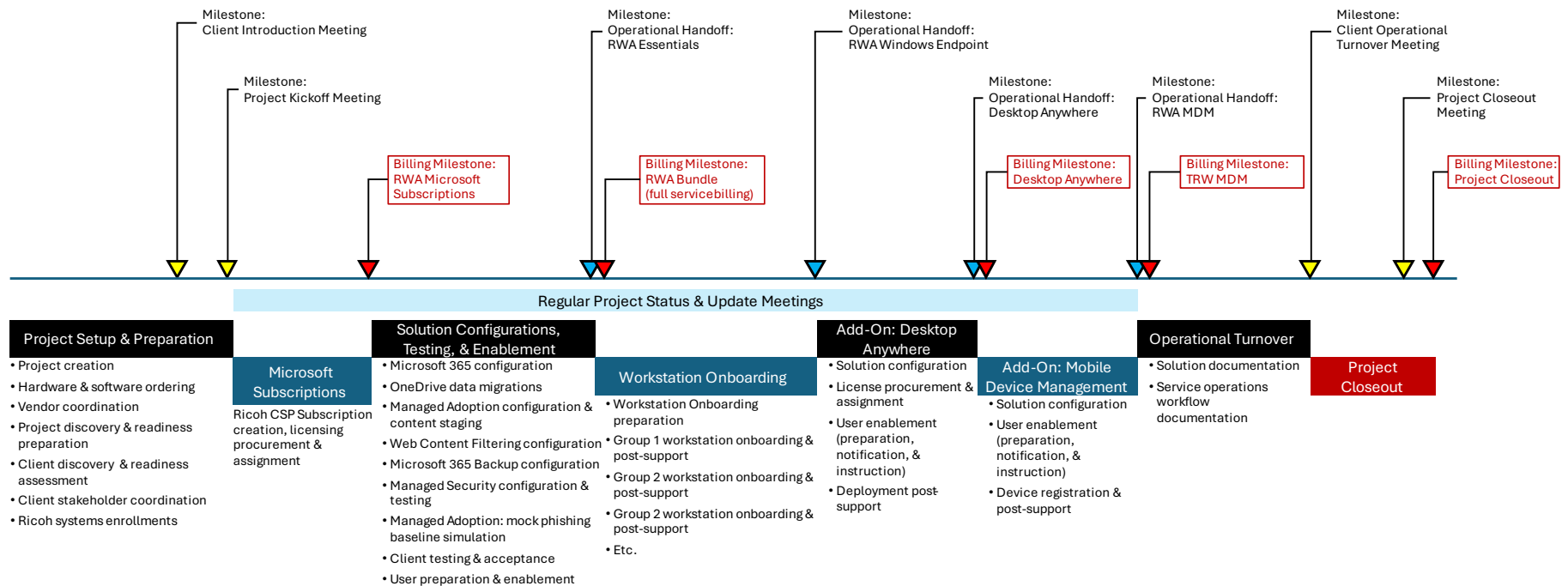
Changes to any part of the SSRC made are subject to Ricoh Service Change Management Governance.

Implementation & Onboarding Timeline

The actual Ricoh Work Anywhere service implementation & Onboarding timeline depends on the service bundle chosen, plus selected add-ons. Other factors that impact the implementation and onboarding timeline include:

- The size and complexity of the company
- Scheduling considerations
- Other Ricoh services ordered by the client
- End user and resource availability
- Device compatibility with Ricoh Work Anywhere solutions
- And more

An example progression timeline for a typical Ricoh Work Anywhere implementation and onboarding is shown below. Note that project and billing milestones are defined in the timeline.



Glossary of Definitions

1. **Service Offering (or Service):** The services and solutions provided and managed by Ricoh.
2. **Service Solution:** The functional technology solution that underlies the service offering. This may consist of one or more solutions working together from different solution providers.
3. **Client Representative:** Also known as client Point of Contact (POC). One or more designated representatives of the client organization who are stakeholders who can make decisions on day-to-day IT operations of their company committed to promoting successful business outcomes of the service. Client Representatives have authority to make service requests to Ricoh on behalf of their company. Client Representatives can authorize requests made by users within their organization to Ricoh.
4. **End User:** Client employee, worker, approved guest, or approved contractor working directly with the services described in this document within the client's network & domain on a full time, part time, or temporary basis.
5. **Inactive User:** An end user account is considered inactive when the client requests a stop/pause on the user account services and activities, and Microsoft licensing has been unassigned from the user account.
6. **Endpoint:** Physical devices that connect to and exchange information with a computer network or networks. In the context of Ricoh Work Anywhere services, endpoints are laptop or desktop workstations, mobile phones with Internet and app capabilities, and mobile tablet devices.
7. **Company Endpoint:** An endpoint device owned and operated by the company specifically for company use, either assigned to a specific user or available for shared use by multiple users.
8. **Personal Endpoint:** An endpoint device owned and operated by a user for primarily personal use.
9. **BYOD:** An acronym for Bring Your Own Device, the ability for a user to utilize their personal endpoint for company use without sacrificing functionality, privacy or security. BYOD use usually requires company authorization and a formal terms of use policy issued by the company and agreed to by the user(s).
10. **Operating System:** The root software on an endpoint device that runs the hardware and essential functions of the device. Operating Systems include but are not limited to Windows, Apple OS, iOS, and Android.
11. **Windows Desktop:** The graphical interface presented to users when launching and operating a Windows workstation endpoint.
12. **Mobile Application Management (MAM):** The ability to manage business mobile apps on company-provided and personal mobile devices.
13. **Mobile Device Management (MDM):** The ability to manage a company-provided mobile device and its installed applications.

14. **Managed Active Directory:** Client's private Active Directory Domain environment wherein Ricoh provides Server Management for all of the Domain Controllers that constitute the Active Directory Domain.
15. **Unmanaged Active Directory:** Client's private Active Directory Domain environment wherein Ricoh does not manage the Domain Controllers that constitute the Active Directory Domain.
16. **Azure Active Directory:** (aka Microsoft Entra ID): Cloud-based Active Directory Services provided by Microsoft as part of the Microsoft 365 cloud business solution.
17. **Hybrid Active Directory:** An environment composed of a private Active Directory Domain operating in conjunction with an associated Azure Active Directory Domain. See Appendix B for details and Best Practices concerning Hybrid Active Directory.
18. **Backup:** The process of capturing a copy of data from an active production system or platform (aka Source) and storing said data on a different platform so it can be used for restore/recovery in the event the primary data is lost or becomes unusable. Backups are conducted in regularly-scheduled sessions.
19. **Restore Point:** Point-in-time data captured by a backup session. Backups of any data source contain multiple restore points captured over time, providing a chronological history of the data for restore purposes.
20. **Restore:** The process of copying data from a selected backup restore point to a defined destination. The destination can be "In-Place" (replace/overwrite data on the active production system/storage), or "Non-Destructive" (a non-active platform). Restore sessions are conducted on an on-demand basis as an Administrative Request.
21. **Incident:** Report of failure, unplanned interruption, disruption of access, or reduction in quality or functionality of Ricoh Work Anywhere services.
22. **Incident Submission:** Incidents are submitted by end users or the Client Representative to Ricoh Support as defined in this document.
23. **Problem:** Underlying cause of an incident. May be resolved as part of the reactive incident support process; or may require more extensive resolution via engineering.
24. **Administrative Service Request:** Non-incident requests for changes to the Steady-State Running Configuration for End Users.
25. **Administrative Service Request Submission:** Service Requests are submitted by the authorized Client Representatives to Ricoh as described in this document and can be processed without Change Control Management process.
26. **Service Configuration Change Request:** Non-incident requests for changes to the Steady-State Running Configuration that affect many or all users in the client organization, requiring assessment, planning and testing prior to formal implementation into the solution/service.
27. **Service Configuration Change Request Submission:** Service Requests are submitted by the authorized Client Representatives to Ricoh as described in this document and are subject to Ricoh Change Control Governance.
 - a. Ricoh may deny the change request as it may compromise the integrity of the service solution design, security, or otherwise.

- b. Ricoh may determine that a service fee is required to implement the change request.
 - c. Ricoh may identify the change request as a feature that is provided by a higher level of service, and may suggest the client upgrade to the higher service level.
28. **Service Lifecycle:** Ongoing changes & improvements to the core business solution and associated Ricoh managed IT services as defined in this document. Service Lifecycle changes may be mandated by the business solution provider or by Ricoh.
29. **Service Lifecycle Event:** Ricoh will identify, review, and submit Service Lifecycle Events for review. Events are subject to Ricoh Change Control Management and will be planned, tested, and approved prior to general implementation for our clients.
30. **Service Monitoring:** The process of collecting performance data from constituent system or device sources used for the purpose of detecting Monitoring Events. Ricoh determines what sources are used and data collected for Service Monitoring purposes. Collected data does not include user credentials, file content, or other business-related data.
31. **Service Monitoring Event:** An observed change in Service Monitoring. Service Monitoring Events may have no impact to the service, or may result in an actual or potential service disruption for one or more users. Ricoh determines the types of Service Monitoring Events that are detected and the conditions that define their criticality and priority in service continuity.
32. **Service Monitoring Alert:** Notification that a Service Monitoring Event has occurred. Alerts may be sent to Ricoh service management teams, to the client, or both. Alerts may report actual disruptions to service continuity or may be predictive so that action can be taken proactively to avoid service disruption. Ricoh determines which Service Monitoring Events generate Service Monitoring Alerts, and recipient(s) of the Alerts.
33. **Steady-State Running Configuration:** The standardized service solution configuration as designed and implemented by Ricoh.
34. Incident and Service Request types and conditions not stated in this Service Description are considered out-of-scope of this Service Description.