RPOST

SERVICE LEVEL AGREEMENT

Securing Email and Digitizing Workflows

RPost is a global leader in secure and certified electronic communications, built upon its patented RMail®, RSign®, and Registered Email™ delivery proof, email encryption, e-security, and e-signature technologies. Millions of users have enjoyed RPost services in more than 100 countries, since 2000.

Standard Service Level Agreement

This Service Level Agreement governs all RPost messaging and document services currently commercially available. If there is another reference that conflicts with a definition in this Service Level Agreement, the definition or description within this Service Level Agreement prevails, unless a customer specially contracts for a different service level in a separate contract.

Contents

I. Definitions:

1. **RPost® Systems.** All RPost software service systems, API, and connected applications that process or route customer messages and data.
2. **RMail® Platform.** RPost software service systems that process RMail services, subsets, and related services unless otherwise specified, including but not limited to Registered Email™, email encryption, RSign Lite (a/k/a RMail E-Sign), File Share (a/k/a LargeMail), SideNote®, Anti-Whaling services and some versions of RForms.
3. **RMail Gateway™.** Local application or cloud managed service for filtering email content outbound prior to RMail Platform processing, inbound, or archive.
4. **RSign® Platform.** RPost software service systems that process all RSign e-signature services other than RSign Lite (a/k/a RMail E-Sign) and some versions of RForms.
5. **R1:** RPost infrastructure for standard volumes and human sending.
6. **R2:** RPost infrastructure for automatic and high volume sending.
7. **Service.** Services enabled by RMail Platform, RMail Gateway, RSign Platform, or RPost Systems.

II. RPost General Services:

1. Service Availability. RPost guarantees 99.9% availability for 24 x 7 Service operation without severity level 1 disruption, excluding scheduled maintenance windows.

2. Scheduled Maintenance Outages. Planned, scheduled maintenance outages are limited to a specific window during off-peak hours. Customers and alliance partners will be notified of planned outages in advance. Off-peak hours have a target maintenance window start time of 1am UTC, with variation for off-peak if the maintenance only affects geographical regional systems.
3. Time to Intervene. RPost support ticketing is available 24×7. Reported incidents are required to be logged with a support ticket through a system available on RPost corporate and product marketing websites. RPost support ticketing system provides information related to ticket status. The mean time to investigate basic support plan support tickets is 48 hours based on a 24-hour business day. The mean time to investigate enhanced support plan support tickets is noted in the Premium Support Enhancement section. Tickets that are received and clearly identified as Service Incident Severity Levels 1, 2, 3 and 4 in the Ticket Subject are verified within a mean time of 6 hours of submission with basic support plans and if confirmed as Severity Levels 1, 2, 3 and 4 issues, are responded to within the timeframe noted in Time to Restore.
4. Time to Restore. The mean time to restore from time of identification of any unplanned generalized service outage or Service Incident Severity Levels 1, 2, 3 and 4 is six hours.
5. Time to Change. The mean time to respond and/or implement automatic change requests is one business day. The mean time to respond and/or implement manual change requests is one business day. Completion time for such requests will be subject to the nature of the request.
6. Support Enhancements. RPost offers premium support options that provide enhancements to the above.
    a. *Enterprise Support:* Customer has the option to immediately escalate all support tickets to level 3 support for senior manager investigation and oversight. Mean time to intervene is 6 hours**.** The mean time to restore after support ticket submission is 6 hours and if VIP escalated, 3 hours from VIP escalation.
    b. *Platinum Support:* Mean time to intervene is 12-hours. The mean time to restore after support ticket submission is 12 hours.
    c. *Premium Support:* Mean time to intervene is 24 hours. The mean time to restore after support ticket submission is 24 hours.

7. Service Incident Severity Definitions and Notices.
    a. *Definitions*
        i. Severity Level 1: Total loss of all services, e.g., no users on the network can access any services. For example, no user can send any messages through RPost systems from any of its infrastructures or with any feature.
        ii. Severity Level 2: Total loss of a main service for a specific region, e.g., no users on the network in a region can access a main service, with main service defined as Registered Email™, encrypted email, file transfer or e-signature transmission services. Severity Level 2 notices are identified in relation to a specific service function, service infrastructure instance and/or geographic region.
        iii. Severity Level 3: A specific service function is degraded. Severity Level 3 notices are identified in relation to a specific service function or service infrastructure instance. Users can access the service to send but experience difficulties or significant delays of more than two hours. For example, a user sends a message and it is not rejected by the RPost system but there is an extended delivery delay beyond mean time parameters for service functions, such as a delayed return of the Registered Receipt™ email beyond the mean time to return.
        iv. Severity Level 4: Services are delivered with difficulties or delays of less than two hours. Users accessing the service are not significantly impacted. For example, a user sends a message and there is an intermittent delivery delay beyond mean time parameters for service functions.

        v. Unauthorized Information Disclosure: Unauthorized disclosure of information that resides on the service processing systems that becomes public which is considered protected personal information or customer private information under privacy regulatory frameworks of HIPAA, GDPR, or applicable local privacy regulations that govern such data.

    b. *Notices:* RPost service operations center shall report to affected users with an email notice or by other contact means within a mean time to respond of 72 hours after initial awareness of a service related issue of Severity Level 1, 2, or Unauthorized Information Disclosure, with such notice providing a summary of the issue, duration of the issue, resolution of the issue if resolved, actions to mitigate re-occurrence of the issue if known, and impact of the issue with the best information that the knowledge of the RPost operations staff at the time of the notice is able to obtain.

8. Service Provisioning.
    a. *Self-Provisioning Default Plans.* RPost services may be self-provisioned for limited ongoing use through select user interfaces including Microsoft Outlook, Gmail and web apps ("Default Use"). Services are immediately available for Default Use.
    b. *Corporate Provisioning.* RPost services may be provisioned in highly specialized scenarios and with systems integrations including connected to third party systems, volume sending systems, or apps such as Salesforce.com that may require administrative provisioning and corporate orders on business service plans ("Business Orders"). Customers using these specialized provisioning systems may need to be enabled or approved by RPost staff or RPost partner staff after order submission. RPost mean time to process Business Orders is one business day.
    c. *Service Enhancements.* Throughout this Service Level Agreement RPost may describe capabilities only available to users that are on select service plans or may elect for service enhancements. RPost reserves the right to require fee-based service enhancement packages or premium service plans for access to certain services, settings, or parameters described in this Service Level Agreement. Not all customers may have access to all of the services described in this Service Level Agreement or in other service plan or service description materials, service parameters, service levels or enhancements but may inquire how to obtain access should they so desire.
9. Service Operations Verification.
    a. *Deliverability Testing.* It is the customer's responsibility to ensure sent message traffic has proper deliverability and to request whitelisting, SPF and/or DKIM set-up as the customer may desire (and to test DKIM configurations after set-up) and report DMARC policies that need special attention.
    b. *Service Settings.* It is the customer's responsibility to ensure service parameters are as the customer desires, including setting minimum encrypted transmission levels and other retention parameters.
    c. *Proper Installation in Customer Environment.* It is the customer's responsibility to ensure that the service has been installed and is in proper function within its technology environment, including testing the Registered Receipt™ verification process to ensure the customer's anti-virus systems are not altering these receipt emails in a manner that invalidates the authentication process, and including testing message delivery and return receipt and report functionality to ensure the customers' anti-spam systems do not block RPost system message traffic. RPost offers options to support customers that need to mitigate any issues related to service operations with anti-virus and anti-spam systems including whitelisting information or use of the RMail Gateway pre-configured anti-virus and anti-spam services.
10. Message Delivery Time. Under normal service operations on R1, RPost service messages will be processed (sent from the sender's server and received by the R1 RPost processing server) and sent for delivery within a mean time of five minutes of induction by the RPost service. Acknowledgement™ receipt emails will be returned within a mean time of ten minutes after message induction by the RPost service after authentication of sender accessibility. Registered Receipt™ emails will be returned to the sender within a mean time of 2 hours from the

original message induction by the RPost service (the time inducted as reported on the Acknowledgement receipt). The above timeframes are valid for 99% of deliveries on R1. R2 mean times are double those of R1 due metering for optimal deliverability of volume batch sends. RPost is not accountable for delays caused by external factors such as Internet network outages, Internet network congestion, sender or recipient mail server failures and/or incorrectly addressed messages, or third-party delays for customer requirements of Registered Receipt™ processing to include locally sourced third-party API retrieved timestamps.

11. Undeliverable Message. In the case of undeliverable messages sent for RPost service processing, the service may attempt to deliver the message through alternate servers (depending on the sender geography and service plan) and if ultimately undeliverable, the service will return an interim notice to the sender if such delivery failure can be determined conclusively upon the first send attempt, and the service will follow with a complete Registered Receipt™ email or other service report to the sender within above time parameters for Registered Receipt™ email and as per schedule for other service reports, depending on the type of status poll or reports. After a reported undeliverable message, RPost services have no additional responsibility to attempt to re-deliver the undeliverable message. It is solely the responsibility of the sender to resend messages. The RPost service operations considers a sent and undeliverable message as a consumed service Unit or Units as if the message had been delivered, with the number of consumed units based on the normal Unit calculation based on service feature, number of recipients and message sent size.
12. RPost Testimony. If the validity of a Registered Email™ receipt or the service is questioned in a legal proceeding, RPost may make in-house or third-party experts trained in the operation of the RPost service available to give testimony at a cost not to exceed a rate of $550 per hour, plus reasonable customer pre-approved travel and other expenses.
13. Reporting. RPost may provide monthly usage reports to individual users that present each RPost service Unit with detail including the time sent and the recipient destination. RPost may provide aggregate reports to corporate account administrators and alliance partners as requested. None of these reports contain message body text or attachment content but may contain message header information and message delivery metadata. RPost provides options for a right to be forgotten and levels of data masking which, if opted for, may limit the data available or viewable in its service reports. Review the RPost privacy policy notice for further information.
14. Whitelisting. RPost makes available at support.rpost.com information for whitelisting messages sent from the RPost System. It is the obligation of the customer to employ these whitelisting options for service functionality.

15. Service Plan Definitions.

    a. *Term Expiration:* 23:59 UTC on the last day of the period (month or year).
    b. *Term Renew:* Reset on the first day of each calendar month at time zero (UTC).
    c. *Individual Plans:* Service authorized for one human sender from one sender email address. Examples of these plans are RMail 365, RMail Standard, RMail Business, RSign 365, RSign Standard, and RSign Business.
    d. *Shared Volume:* Service authorized for finite set of associated email address senders and period message volume authorized for the plan, within one sending company. Examples of these plans are RMail Shared Volume Monthly 10K and RSign Shared Volume Annual 10K.
    e. *Maximum Users:* Maximum sender email addresses that may be associated with a Shared plan.
    f. *Qualified Plan:* Individual plans that require a minimum number of plans to be purchased within a sending company. Examples of these plans are RMail Business, RMail Enterprise, RSign Business, and RSign Enterprise.
    g. *Premium Plans:* Individual plans that qualify for special benefits if ordered in volume in some situations. Examples of these plans are RMail Standard, RMail Business, RSign Standard, and RSign Business.

h. *Fixed:* Service shuts off when the plan message allotment in the period (month/year) has been reached. Users may upgrade plans at any time. If no upgrade is available, the user will need to contact their account manager or switch certain users to a different plan or a shared volume plan.

i. *Service Plan Message and Unit Expiration:* For Monthly plans (Individual plans that have message units reset monthly and Shared Volume monthly plans), unused units expire every month; for Shared Volume Annual plans, unused units expire after 12 months from the service plan availability date or as used if used sooner.

16. Units of Measurement.

a. *RMail Unit.* Each recipient destination per 5-megabyte message size is one Unit, whether deliverable or undeliverable.

   i. RMail E-Sign and Register Reply. Each Register Reply™ or RMail E-Sign (a/k/a RSign Lite) message counts as two Units for each recipient destination per 5-megabyte message size to account for the message sent and the availability of the reply recorded, whether replied to or e-signed, or not replied to or e-signed.

   ii. File Share. Each recipient destination per 100-megabyte message size is one Unit.

   iii. Encrypted Reply. Each recipient destination is permitted five encrypted replies and is considered one message Unite per recipient destination per 5-megabyte message size.

   iv. Default Plan. For each sent message under the default service plan, one Message Unit may include up to 10 recipients and may be up to 25MB.

   v. Authentication of Registered Receipt™ Email. Each automated authentication of a Registered Receipt™ email record is one Unit; except for extra-large Registered Receipt™ email record authentication (defined as Registered Receipt™ file size greater than 15 MB) which is five Units.

b. *RSign Unit.* Each message envelope comprising up to 25 recipients and per 25 MB message size is an RSign Unit (other than abovementioned RMail E-Sign (a/k/a RSign Lite usage).

17. Default Service Parameters. Refer to the support references for Default Service Parameters of the RMail Platform and RSign Platform. Refer the RPost Billing Guide (available upon request) for further details on service and plan parameters and accounting for use. These service parameter reference pages are incorporated by reference. The Default Service Parameters Notice is available at rpost.com.

18. Fair Use Policies. Fair use policies apply to all plans, and include limits per plan, limits per send, non-use for unsolicited marketing purposes, and non-use for unlawful transmissions. RPost reserves the right to terminate service or to temporarily freeze the user's account and/or contact the user or their administrator to verify if traffic is authentic and determine if the particular user's plan parameters should be adjusted. RPost reserves the right to change this Fair Use Policy at any time. Changes shall become effective after thirty (30) days of publication of the revised version on rpost.com. Continued use of a subscription after expiry of the 30-day period shall constitute acceptance to be bound by the terms and conditions of the revised fair usage policy. Refer to the Fair Use Policy notice available in the rpost.com for further details.

19. Privacy Policies. All RPost services, including RMail and RSign, are governed by the RPost privacy policy notice incorporated by reference. The Privacy Policy Notice is available on rpost.com.

20. Administrator Access. All RPost services provide the customer administrator access to some service data or metrics that may be useful to manage the customer account. It is the responsibility of the customer to determine who should be provided and who should be limited from having customer administrator access privileges. RPost provides various enhanced security options and it is the responsibility of the customer to request non-default settings or settings that limit access to customer administrators or other users. These defaults and settings vary depending on service app, interface, service plan, and/or service function.

21. Recourse for Breach. If RPost is found to be in a material breach of this Service Level Agreement that caused quantifiable damage to a customer user, with that customer and user properly using the service within the Fair Use Policies and properly paying fees in compliance with a personal or business service plan and its plan parameters ("Breach"), RPost shall have liability limited to the amount paid for those RPost messages damaged by such Breach on a pro-rata basis, based on payments made for service and service use over the prior annual period or if there is not yet an annual term for the customer and user, the average prior months payments made for service and service use since customer and user inception whichever is shorter. RPost shall not have liability for Breach for service users that do not fall within this definition of Breach. RPost shall not have punitive liability associated with service use.

III. RPost Specialized Services

1. RMail System

a. Registered Email™ and its Registered Receipt™ E-Delivery Evidence

i. *Deliverability and Timestamps.* Messages are sent with times recorded for: (a) proof of time of delivery ("POD") which is the time the message that left the sender system was inducted into the RMail system for processing, and (b) proof of time of receipt ("POR") which is the time the message was inducted into the system under the control of the recipient or authorized by the recipient to accept email on their behalf. This POR timestamp can be the time of receipt by the recipient mail server, time the email was placed in the recipient mailbox directory, or time opened at the recipient. RPost offers a special configuration option to suppress detection of opening by recipient systems which is enabled with a default setting and may be adjusted as a service enhancement, based on the desire of a customer administrator. For non-deliveries, the RMail system may return an immediate notice or may return the Registered Receipt email recording the delivery failure. Deliver Failure status is presented to the sender in these receipt emails, and it is the sender's responsibility to contact RPost to further investigate any deliverability issues.

ii. *Accessibility.* Registered Receipt™ emails that are delivered to the sender are purged within the same day of delivery (24-hour period); delivery defined herein by collection or transmission of the Registered Receipt™ email by API to the sending organization or sender controlled systems, or by time of first attempt to transmit the Registered Receipt™ record by email to the sending email address, the sending organization, or sender controlled systems, except (i) if the Registered Receipt™ email has not been collected by the sending organization or sender controlled systems by API, this Registered Receipt™ record shall be retained for a maximum of 14-days, or (ii) if the Registered Receipt™ email has not been deliverable by SMTP to the sending email address, the sending organization, or sender controlled systems (as configured in normal settings or otherwise in the RPortal) on first attempt, the Registered Receipt™ email record shall remain available for delivery retries for a maximum of 14-days from the original send attempt, unless (iii) an alternate arrangement has been established for a specific customer. Registered Receipt™ emails that are larger than the threshold set in RPortal for the feature, "Automatically send Registered Receipt email by LargeMail file share when over this size" will be sent by the RMail File Share service and will be retained for a maximum of 7-days. In the case where the RMail system cannot deliver the Registered Receipt™ email record to the sender due to problems with the sender mail system receiving email address, size limitations, receipt retrieval deficiencies, administrator data entry or otherwise misconfiguration of Registered Receipt™ email destination addresses in RPortal, or otherwise, and if the Registered Receipt™ email record is no longer available, the sender must rely on delivery information (Transaction

Metadata) in the Usage Report for that transaction. It is the responsibility of the user to retrieve their Registered Receipt™ emails before the retention time periods expiration.

iii. *Authentication.* Registered Receipt™ email records may be automatically authenticated by an active service user or their designee while the service user who sent the original message that generated the Registered Receipt email record maintains a commercial fee-for-service plan with automatic authentication and a properly maintained Registered Receipt email record. Once a service customer cancels their service account or ceases to pay fees due, RPost does not have any responsibility to continue to provide authentication services. RPost has no obligation to authenticate the same Registered Receipt for more than ten authentication requests or for more than seven years from original creation, although it may do so at its sole discretion. Users may use their own experts to authenticate the receipt information at any time. Users may request RPost to provide additional receipt authentication services at any time and RPost reserves the right to charge additional fees for such additional authentication services or authentication services for cancelled customers. For service users that received a Registered Receipt email record while using a Default and Trial service plan, while RPost generally provides automatic authentication services for those Registered Receipt emails generated during Default service plan use within the parameters mentioned above with no fee for service requirement, RPost has no obligation to authenticate any Registered Receipt email sent with a Default or Trial service plan and may at its sole discretion require a fee for such Default and Trial plan user authentication services.

iv. *Encrypted Content.* Registered Receipt™ email records may be automatically authenticated and is so, reconstruct the original message content. This original message content is not stored by the RMail System. It is reconstructed from data embedded within the Registered Receipt itself. For encrypted messages, the reconstructed message will remain encrypted. It is the responsibility of the customer or customer user to maintain a means to decrypt the reconstructed encrypted message using original encryption passwords or requesting support from RPost to obtain a means to decrypt which is available for active fee-paying service users and may require an additional fee.

b. Registered Encryption™.

i. *Transmission Encryption.* Customer administrators are responsible for selecting the minimum level of transmission layer security that they would like to enforce (current default is TLS 1.0 with options of 1.1, 1.2, 1.3) and, if the minimum set level cannot be met, the system transmission dynamically reverts to an alternate AES 256-bit PDF Message Level transmission method.

ii. *Message Level Encryption.* Customer administrators and/or senders are responsible for selecting the encryption method from sender to system of which default varies depending on the sending app, sender configuration or customer administrator preferences. The default password options default varies depending on the sender app, sender preferences and customer administrator preferences. Customer administrators are responsible for setting any short term encrypted message attachment download alternate options (current default is a 7-day attachment download option enabled, with options to disable any attachment download option or extend the storage for up to 90-days).

iii. *Encrypted Reply.* The reply message and its attachments transmit back to the sender encrypted using the same settings set by the originating message if the encrypted reply service is used.

iv. *Auditable Record of Encrypted Transmission.* The Registered Receipt™ email record provides a fact record of encrypted transmission.

c. Digital Seal® Sent Message Authentication at Recipient.

   i. *Digital Seal Service Requires Seal HTML File.* Recipients of messages sent from senders originating their message and sending with the RMail for Outlook app, other RPost apps with the Digital Seal Sender Authentication, or API and automated sending options specially configured to enable the Digital Seal® service option can verify the integrity of the sent message, original sender address, original content, and original time of transmission so long as the Digital Seal HTML file ("Digital Seal Mark") is available. RPost makes no warranty that the Digital Seal Mark will remain valid in all email systems of all recipients and as that email sent with a Digital Seal Mark is forwarded. RPost makes no representation that a Registered Email™ message with a Digital Seal Mark will have the Digital Seal remain associated with the Registered Email™ message at or after that Registered Email message reaches its first destination. RPost makes no representation that the RPost service will be capable of sending all email, tagged by the End-User for Digital Seal protection, with a Digital Seal. Further, RPost does not claim that the Digital Seal Mark can prove the human identity of the End-User or sender of the Registered Email™ message that has Digital Seal protection.

   ii. *Authentication.* The Digital Seal® Mark may be automatically authenticated by an active service user or their message recipient as long as the service user who sent the original message that generated the Digital Seal Mark maintains a commercial fee-for-service plan. Once a service customer cancels their service account or ceases to pay fees due, RPost does not have any responsibility to continue to provide authentication services. RPost has no obligation to authenticate the same Digital Seal Mark for more than ten authentication requests or for more than seven years from original creation, although it may do so at its sole discretion. Users may use their own experts to authenticate the Digital Seal® Mark information at any time. Users may request RPost to provide additional Digital Seal® Mark authentication services at any time and RPost reserves the right to charge additional fees for such additional authentication services or authentication services for cancelled customers. For service users that sent or received a Digital Seal® Mark email record while using a Default and Trial service plan, while RPost generally provides automatic authentication services for those Digital Seal® Mark emails generated during Default service plan use within the parameters mentioned above with no fee for service requirement, RPost has no obligation to authenticate any Digital Seal® Mark email sent with a Default or Trial service plan and may at its sole discretion require a fee for such Default and Trial plan user.

   iii. *Digital Certificate.* For key accounts and partners that have proper authentication and identity trust chains in place, the Digital Seal® service may be configured to additionally digitally sign an email attached PDF file using a PKI digital certificate and may be additionally configured to digitally sign an email attached PDF file using a digital certificate provided by and uniquely tied to the identity of a sender. While RPost does use best efforts to verify the validity of such a digital certificate provided by a sender, RPost is not the issuer of such digital certificate and relies on the RPost customer to provide RPost a validly issued digital certificate.

d. File Share. File share services store message content for short terms, and after the term, the message content is automatically purged. It is the responsibility of the customer or customer user to maintain the privacy of this content by choosing the encrypted File Share option or otherwise using methods not to publicize the link to retrieve the message or files sent. The RMail system secures the internet connection in the browser and may additionally secure access to the files shared if the encryption option is selected. File(s) are stored for 14-days from when the message was received by the RMail system for processing by default. Customers may request service enhancements to permit changes in storage times with default parameters from 1 to 90 days.

e. RMail Gateway

  i. *Message History Storage.* RMail Gateway default settings include a 7-day cache of message history metadata with no retention of message body and attachment content.

  ii. *Inbound.* Customers are obligated to monitor and manage inbound services in terms of inbound quarantines. All inbound message quarantined traffic is retained in a 7-day quarantine cache.

  iii. *Outbound.* RMail Gateway default settings include standardized packages of message filter and route rules. Customers may request custom filter and route rules that may be considered packages for compliance for various regulations (i.e. HIPAA, GDPR, etc.). While RPost provides standardized rule sets, may suggest standardized or custom rule sets, or may create new standardized or on-demand custom rule sets, RPost does not attest to any rule set guaranteeing compliance with any regulation or requirement, regardless of what the rule set is named or how referenced. It is the customer sole responsibility to determine which filter and route rules are suitable for their business needs, regulations, and/or requirements. Should a customer opt to use filtering policies that block outbound transmission and quarantine outbound messages before transmission, customers are obligated to monitor and manage all their outbound message quarantines. All outbound message quarantined traffic is retained in a 7-day quarantine cache.

  iv. *Archive.* If any RMail Gateway service used is used for message archiving, it is the responsibility of the customer to manage their desired archive retention policies and remain current for fees associated with archive storage. RPost retains the right to purge archived messages after a customer ceases to make timely payments for services or otherwise cancels their service agreement for RPost services. If service fees are less than 90 days past due, RPost shall provide at least one electronically delivered notice with a record of sending attempt, to the last recorded administrator email address associated with the customer account prior to purging an archive. If service fees are more than 90 days past due, RPost does not have any obligation to continue to store data and may purge data without notice.

f. RMail Recommends™. RMail Recommends default settings include standardized packages of message filter and processing rules. Customers may request custom filter and service processing rules that may be considered packages for compliance for various regulations (i.e. HIPAA, GDPR, etc.). While RPost provides standardized rule sets, may suggest standardized or custom rule sets, or may create new standardized or on-demand custom rule sets, RPost does not attest to any rule set guaranteeing compliance with any regulation or requirement, regardless of what the rule set is named or how referenced. It is the customer sole responsibility to determine which filter and service processing rules are suitable for their business needs, regulations, and/or requirements. RPost reserves the right to charge additional fees for use of this service or for users who modify filter and processing rules on their own or with RPost support.

g. API Use. RPost reserves the right to charge additional fees based on the volume of transactions and data transferred using RPost APIs. It is the customer's responsibility to use the API that it may be provided to obtain Registered Receipt and other data records before those records are purged from RPost systems according to the timeframes and parameters associated with each service function. RPost reserves the right to restrict or adjust access to APIs.

h. Transaction Metadata. RPost retains transaction metadata during the billing period associated with each RMail transaction. RPost generally retains RMail transaction metadata (which excludes message body or attachment content) during the contract period associated with each customer. RPost may retain RMail transaction data during the transaction billing period, the customer contract period, and after the customer contract period; however, RPost does not have an obligation to retain RMail transaction metadata beyond the transaction billing period unless specifically contracted for such. RPost provides professional services to permit an individual user (a user who is not part of multi-user customer account) who ceases to continue to use RMail services to request a purge of a that individual's RMail transaction metadata and RPost shall provide such services at no cost to the individual if privacy regulations within the jurisdiction of that individual require such to be free-of-charge. RPost provides professional services to permit a business customer (a customer account with multiple users) that ceases to continue to use RMail services to request a purge of that customer's transaction metadata and RPost offers to provide such services based on an approved professional services statement of work. The content in this Transaction Metadata section does not relate to Registered Receipt™ email record or Digital Seal® email or sender authentication, both of which operate independent the abovementioned retention of transaction metadata.

2. RSign System

a. RSign Lite. RSign Lite (also known as RMail E-Sign) service messages are processed by the RMail System. RSign Lite services do not retain any document records after the transaction processing period ends, which is a default of 30 days after the message was originally sent through the service with configurable parameters up to 90 days.

b. RSign Storage. Customers may opt for the RSign system to store copies of transaction data and completed transactions in a repository available to the customer user or customer administrator. Unless storage enhancements are selected or service plans are activated that dictate longer term storage, RSign Systems will retain information for a minimum of 90 days in live storage and 1 year in archived storage. RPost may at its sole discretion maintain information in live storage or archived storage for longer periods of time so long as it does not exceed the maximum storage period selected by the customer. It is the responsibility of the customer to manage their desired retention policies and remain current for fees associated with storage. RSign transaction data will be maintained for commercial fee-for-service plan users according to these policies. Once a service customer cancels their service account or ceases to pay fees due, RPost retains the right to purge archived transaction data after a customer ceases to make timely payments for services or otherwise cancels their service agreement for RPost services. If service fees are less than 90 days past due, RPost shall provide at least one notice recorded as sent electronically with a record of sending attempt, to the last recorded administrator email address associated with the customer account prior to purging an archive. If service fees are more than 90 days past due, RPost not have any obligation to continue to store data and may purge data without notice. It is the responsibility of the customer to manage their desired retention policies and remain current for fees associated with storage. RPost may continue to retain service billing audit records which comprise of transaction metadata. RPost has no obligation to maintain storage for Default and Trial service plan users or users that access RSign from within their RMail service plan as a Default or Trial service plan.

c. RSign Privacy Modes and Storage Opt-Out. Customers may opt out from any storage of completed transactions. RPost may continue to retain service billing audit records which comprise of transaction metadata. RSign includes three advanced data privacy, masking and deletion settings that may be available to customers based on their geographic location or service plans; and may be relied upon for privacy compliance with the European General Data Protection Regulation (GDPR). These include:

   i. **RSign Private Mode**, which may be enabled (1) on a transaction-by-transaction basis by the end user (at the time of sending), (2) on a transaction-by-transaction basis with a template or rule configuration setting, (3) enabled for all of an individual user's e-sign transactions by default or for a set period of time (when Private Mode is enabled), or (4) enabled for all users in a company account for all e-sign transactions by default for a set period of time (when the setting is enabled). This setting, only for transactions that are initiated while Private Mode is enabled, permanently prevents viewing of a specific RSign transaction document sent for e-signature and e-sign record content, other than for the user initiating the transaction and for the participants in the transaction. It is important to note that this setting is timestamp-transaction dependent meaning Private Mode applies to specific transactions that are initiated at a time when the setting is enabled for a user, or for a transaction that the user applies it to, and it cannot be reversed for that or those particular transactions (e.g. enabling Private Mode permanently prevents a customer administrator access to the content of a particular transaction).

ii. **RSign Masking Mode**, which may be enabled for all customer records and may be disabled at any time by the customer administrator, and while enabled, obfuscates the message transmission data in the RSign interface and prevents record or document download for all records for any user except for the customer administrator and the initiator of the transaction. It is important to note that this setting works like a "toggle" that may be adjusted by the customer administrator and if enabled (Masking On) it will apply to all past and future transactions; if later disabled (Masking Off) it will disable for all past and future transactions. RPost recommends enabling RSign Masking Mode by default for customers that user RSign for transactions across a variety of business groups or business roles within a business group. RSign Masking is compatible with "RSign Private Mode", meaning, a user may select a transaction for Private Mode even if RSign Masking Mode is enabled, meaning that particular transaction be private from that customer administrator per the Private Mode functionality; the Private Mode functionality remaining for that transactions that occurred with Private Mode enabled, even if RSign Masking Mode is later toggled off (disabled).

iii. **RSign Delete Mode**, which permanently obfuscates the message transmission data in the RSign interface and prevents record download for all users including the customer administrator and the initiator of the transaction (other than for the record that the transaction parties receive by email) and auto-purges the transaction record after a pre-defined number of days (7, 10, 14, 30, 60, 90, 180 or 365 days) from the transaction initiation date, with the RPost system only maintaining base transaction metadata for billing records purposes.

1. **Transaction Data and Metadata**: When RSign Delete Mode does not apply, then RPost retains transaction data and metadata during the billing period associated with each RSign transaction. RPost generally retains RSign transaction data and metadata (metadata excludes message body, attachment, or transaction complete content) during the contract period associated with each customer. RPost may retain RSign transaction data and metadata during the transaction billing period, the customer contract period, and after the customer contract period; however, RPost does not have an obligation to retain RSign data or transaction metadata beyond the transaction billing period unless specifically contracted for such. RPost provides professional services to permit an individual user (a user who is not part of multi-user customer account) who ceases to continue to use RSign services to request a purge of a that individual's RSign transaction data and metadata and RPost shall provide such services at no cost to the individual if privacy regulations within the jurisdiction of that individual require such to be free-of-charge. RPost provides professional services to permit a business customer (a customer account with multiple users) that ceases to continue to use RSign services to request a purge of that customer's transaction data (while a customer, via the RSign Delete Mode) or transaction metadata and RPost offers to provide such services based on an approved

professional services statement of work. The content in this Transaction Data and Metadata section does not relate to the authentication capabilities associated with a valid RSign applied digital signature on an RSign transaction record of which operates independent the abovementioned retention of transaction data and metadata.

iv. **RSign End-to-End Encryption Feature**, when used with RSign Privacy Modes and Storage Opt-Out, changes the ability to access unencrypted transaction records as downloads from within the RSign web interface (or API). Transaction record content will be accessible for viewing and download without a password associated with that transaction record after log-in to the relevant RSign account unless RSign Privacy Modes and Storage Opt-Out options maintain the privacy, masking, or deletion of that particular transaction or views per these settings.

v. **RSign API Record Retrieve**, when used with RSign Privacy Modes and Storage Opt-Out, will only retrieve transactions that would be permissible to view under the user's (API key user's) permissions per the RSign Privacy Modes and Storage Opt-Out options associated with the user or the transaction.

d. API Use. RPost reserves the right to charge additional fees based on the volume of transactions and data transferred using RPost APIs. It is the customer's responsibility to use the API that it may be provided to obtain transaction data and other data records before those records are purged from RPost systems according to the timeframes and parameters associated with each service function. RPost reserves the right to restrict or adjust access to APIs.

Last Update: 210323