Arctera™ Unified Platform Service Description

Service Overview

The **Arctera Unified Platform Services** (“Services”) deliver a SaaS-based solution for Archiving, eDiscovery, and Surveillance via an All-In-One SKU as detailed in this service description (“Service Description”) Documentation.

Arctera Unified Platform - Capabilities

- Archiving
- Capture
- Classification
- eDiscovery
- Surveillance

Arctera Unified Platform - Considerations

Data Import/Ingestion: The Data Import/Ingestion allows Customer to migrate and ingest existing legacy Email data into Customer’s archive, combining both ingested legacy Email and new Email streams within the archive. All work is done remotely. If Customer is moving from an on-premise Enterprise Vault environment, Company will use Direct Migrator as part of the ingestion process, a feature within the Service, to move that data into the Service archive.

For Direct Migrator ingestions:

- Customer’s Enterprise Vault environment must be in stable and working order, including all indexes if applicable, prior to these Services.
- Company requires independent remote access to the Enterprise Vault and extraction environment such as via VPN or Citrix to the migration and SQL servers
- Decommissioning the existing legacy Enterprise Vault environment is out of scope for these Services.
- Please see the Direct Migrator for Enterprise Vault and M365 section, as applicable, for more details around Company’s and Customer’s responsibilities during the Direct Migrator process.

For all other ingestion activities:

- This Service requires active participation by Customer to plan, analyze and execute an ingestion plan.
- Customer must transfer Email data to be ingested via SFTP where applicable and available.
- Customer can extract the data and provide it in any compatible format from supported repositories.
- With Customer’s guidance, this Service assigns Users to each Email imported. Emails that cannot be directly assigned to a specific User are assigned to a single mailbox within the archive. Once an item is assigned to this mailbox, it cannot be moved or migrated to another mailbox.
- All migration activity can be logged and audited through a chain of custody protocol to provide integrity of Customer’s Email records.

- Company cannot guarantee the time it will take to import the data once received.

Company is not responsible for failure to import data that is corrupt when received from Customer.

Customer understands that any Data Import/Ingestion will take considerable time, will run concurrently with the Services Customer has purchased, and that Customer will be able to access and use these other Services purchased in the meantime in accordance with this Service Description. Customer acknowledges and agrees that it is not entitled to any refund or discount on these Services for any time taken or delays encountered with the delivery of the Data Import/Ingestion.

Customer has thirty (30) days following the completion of the migrated data ("Migrated Data") to review, fully test, and provide written notice of and reason for rejection of any Migrated Data or some portion thereof. Upon such notice, Company shall work with Customer to plan and perform any reasonable corrective action. If Company cannot provide the corrective action, Customer and Company agree that no further remediation is required, and Customer is released from payment for that portion of the rejected Migrated Data. Customer is not released from payment for any Migrated Data that has not been rejected within the 30-day period. This is the sole and exclusive remedy for any rejected Migrated Data.

Data Export/Extraction. Data Export/Extraction is provided solely as a Customer self-service capability, and is only available during an active Service term of the Agreement. Company reserves the right to limit extraction requests if the volume of requests is degrading the overall service experience for Company's other customers. Please note Customer's access to the Service in all capacities including extractions ends with the Service expiration, suspension or termination. Customer data is deleted permanently 30 days after the end of the Service term.

Customer Responsibilities

Company can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Company's performance of the Service may be delayed, impaired or prevented and/or eligibility for Service Level Agreement benefits may be voided.

- **Setup Enablement:** Customer must provide information required for Company to begin providing the Service.
- **Adequate Customer Personnel:** Customer must provide adequate personnel to assist Company in delivery of the Service, upon reasonable request by Company.
- **Customer Portal:** Customer can access a web interface Service portal by using a secure password protected login. This Service portal provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service. Customer must configure the features of the Service through the web interface Service portal or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control.
- **Unassigned Licenses:** The Unassigned Legacy Folder plays a critical role in ensuring the Customer compliantly captures all messages flowing into its Service archive, even if a new User hasn't been provisioned within the archive yet. This folder captures all messages that do not match an existing email address provisioned within the archive. Administrators are encouraged to

review the contents of the folder on a regular basis to confirm that all messages are being properly archived. This folder counts as one User in the Customer's total number of Users since the messages contained in the folder consume storage space within the archive.

- **Mail Reassignment:** Mail reassignment allows an administrator in a Customer's archive to reassign unassigned legacy accounts, saved searches, and tags in a self-service fashion up to the limits as detailed at https://supportarctera.cloud.com/support-home/kbsearch/article?articleNumber=100049582

- **Electronic Discovery Capabilities:** Customer may perform electronic discovery requests on its Customer Data to extract an offline copy of that request. However, for Company to preserve the integrity of the Service, maintain its Service Uptime commitments and align with industry standards, these discovery requests are limited per job and per period. Company reserves the right to limit or even refuse discovery service requests if the volume of requests is degrading the overall service experience for Company's other customers, or otherwise doesn't align with the Acceptable Use Policy.

- Compliance: Customer is responsible for all activities that occur in User accounts and for its Users' compliance with the Agreement and with the Acceptable Use Policy, provided at the end of this Service Description. If Customer becomes aware of a User's violation of the Agreement or Acceptable Use Policy, Customer must notify Company as soon as reasonably practicable.

- Security Vulnerability or Incident. If Customer becomes aware of any actual or potential security vulnerability or incident, Customer must immediately report it to Company.

- The Service does not replace Customer's need to backup Customer's mail server(s). If Customer needs to rebuild a mail server, they should rebuild the mail server from backup data rather than from the archive.

- By default, Company automatically generates and stores a unique encryption key for each customer at the time of provisioning to protect Customer Data. If Customer chooses to provide Company with its own encryption key for encrypting Customer Data, Customer is solely responsible for (1) providing Company with access to that encryption key during provisioning in order for Company to be able to provide Service (Service cannot be provided without such access), and (2) independently storing and backing up that encryption key, as ALL CUSTOMER DATA WILL BE LOST AND IRRETRIEVABLE IF CUSTOMER'S ENCRYPTION KEY IS LOST. Customer may revoke Company's access to its encryption key at any time, but in the absence of a material breach by Company to be handled by the parties in accordance with the terms of the agreement, Customer will remain responsible for any pre-committed term and associated fees.

    - Please note that metadata related to Customer Data, such as indexing, database information, or log files will still be independently encrypted with a separate Company-managed key.

    - Company cannot retroactively apply a new encryption key to Customer Data in an existing Tenant. Please reach out to Company for paid-for migration services to move existing Customer Data to a new Tenant that uses Customer's own encryption key.

Direct Migrator Services for Enterprise Vault and M365

Overview

Customer must be moving from an on-premise Enterprise Vault or M365 (Exchange Online) environment to Arctera Unified Platform to be eligible for Direct Migrator Services. Company will use Direct Migrator as part of the ingestion process to move that data into the Service archive.

Scope

The scope of these Services covers the migration of the following types of data to Arctera Unified Platform:

- Enterprise Vault
    - Customer's Enterprise Vault data in supported archive types per the Admin Guide up to the maximum number of gigabytes ("Maximum Migration Threshold") specified in the Services Instrument for Data Import/Ingestion and Storage (typically, the quantity of gigabytes called out in an authorized quote, PO, and/or other service order document)
    - Discovery Accelerator and/or Surveillance (aka Compliance Accelerator) work product as defined in the Admin Guide
- M365
    - Customer's email data in supported mailbox types per the Admin Guide up to the maximum number of gigabytes ("Maximum Migration Threshold") specified in the Services Instrument for Data Import/Ingestion and Storage (typically, the quantity of gigabytes called out in a Quote, PO, and/or other service order document).

Note

The Maximum Migration Threshold is generally set forth in the Customer's purchase order as the amount of data to be imported and is based upon the amount of data that needs to be sent to the SaaS Service for importing/processing ("Data Imported") and storage. Estimating this amount is best done by using the Enterprise Vault Collector Agent's Scan Enterprise Vault Data feature, as described in the Admin Guide, and adding up the items to be captured for all archives to be migrated (either ItemsOriginalSizeInMB or FilteredItemsOriginalSizeInMB).

Functional Requirements:

Environment - Enterprise Vault

- Customer's Enterprise Vault environment must be in stable and working order (including any indexes if applicable) prior to Company beginning the implement phase . If not, Customer must repair the environment before the migration begins.
- Customer is responsible for maintaining current product support & maintenance agreements for all software and hardware in the Enterprise Vault environment during performance of these Services.

Environment - M365

- Customer shall provision and/or administer systems, OS, DNS, user/service accounts, applications, storage, networking, DNS records, and DNS aliases.
- Company requires independent remote access to the Enterprise Vault and migration environment such as via VPN or Citrix to the migration and SQL servers.
- Customer shall provision and/or administer systems, OS, DNS, user/service accounts, applications, storage, networking, DNS records, and DNS aliases.
- Company requires independent remote access to the migration environment such as via VPN or Citrix to the migration and SQL servers.
- To run the M365 Collector Agent application, a typical installation uses a single SQL Server and multiple Agent servers with M365 Collector Agent services installed. For a collection of 500 mailboxes or less, 1 agent node is sufficient. Exact recommended count will be determined during migration planning.

Planning

- Customer shall present documented Enterprise Vault SQL and application maintenance plans and other planned outages to Company project team.

Implementation

- Customer is responsible to finalize pre-requisites prior to Company beginning the Implement phase and migration activities.
- Customer shall manage legal holds and inform Company of any Discovery Accelerator/ Surveillance (aka Compliance Accelerator) work products that need to be migrated.
- Customer shall track, resolve, and document unplanned Enterprise Vault SQL or application outages as such events might impact the overall migration timeline and completeness if they occur.
- Multiple attempts will be made to process failed messages. If it is determined these messages cannot be migrated, the failed messages will be reported as an exception and a report outlining the failed messages will be generated and provided to Customer at the end of the migration.
- If extracted data totals increase beyond those purchased by Customer per the Services Instrument, the parties shall execute a Change Order to address the handling of any extra data
- Customer must keep Company's remote access capabilities to the Enterprise Vault and migration environment running at all times
- Company will provide project management services to manage Company's own activities according to the implementation plan. If Customer requires more comprehensive project management services for the overall project, then the customer must provide these project management services.

Key Dependencies

Prerequisites, assumptions, or dependencies for the Service is:

- The Service is provided directly to Customer and is not available for partners or service providers acting on behalf of a Customer without Company's prior written consent.

- All work to be performed from a Company approved remote facility during normal U.S. working hours. Company's support services may assist after hours at Company's discretion.
- Customer shall provide independent remote access to the Enterprise Vault and migration environment such as VPN or Citrix for any applicable environments and keep it running at all times during the performance of Services for at least two migration engineers 1) primary, 2) backup.
- Customer may require Company migration engineers to attend training sessions prior to Customer providing remote access to its Enterprise Vault and migration environment. Such training sessions shall be limited in scope strictly to what is required and in no event exceed three (3) hours per engineer.
- Customer is responsible for the following tasks:
    - Customer's change control process.
    - Coordinating resources to assist Company with environment access and engagement tasks.
    - Disclose any known issues with the legacy Enterprise Vault environment.
    - Disclose any known issues with the legacy data that was moved into M365, failed items, special scripts for imported PST files, MSG or EML conversions etc.
    - Provision the necessary server and database infrastructure, as agreed with the Company migration engineer, in conformance to the system requirements in the Admin Guide.
    - Company recommends that prior to any migration, Customer should back up the environments.
    - Retiring the existing legacy Enterprise Vault environment is out of scope for these Services.
    - Changes to the scope may be made with written change requests agreed upon by Company and the Customer.
    - Troubleshoot and resolve any configuration issues on Customer's side that are adversely affecting the overall speed of the data migration process.
    - If Customer migration and data import exceeds the Maximum Migration Threshold, parties will execute a Change Order for any additional fees for the additional data import and/or storage beyond that Maximum Migration Threshold.

- Company estimates that its personnel will require approximately twelve (12) hours of setup time and about two to three (2-3) hours per terabyte migrated ("Maximum Company Personnel Hours"). Should Company exceed this amount of time, Company reserves the right to stop migrating any new data, reduce the amount of interaction with Customer, or otherwise require a Change Order to continue providing Services. If Services are being provided to Customer free of charge, or some portion thereof are, Company reserves the right to further limit its Maximum Company Personnel Hours in its sole discretion for such free Services.
- Licenses: Customer shall ensure that prior to the commencement of Services by Company and continuing throughout the provision of Services, that: (i) all the necessary Company software products have been correctly licensed for all appropriate platforms (and all required versions) and the same are made available, in a timely manner, to Company; (ii) the operating systems of all appropriate servers and computers shall be at a level supported by the Company software products to be used; (iii) the storage configuration is a formally qualified configuration for the Company software products to be used; (iv) the technical environment, including the application and database environments, shall be kept under change control and that the physical environment is stable and provides a viable environment for the Company consultants to

undertake the Services; and (v) third parties such as Internet Service Providers have been made aware of any applicable testing that might be carried out by Company. Payment for, license, use and operation of all software and/or hardware products are the sole responsibility of Customer. Customer acknowledges and agrees that no Company software and / or hardware products shall be provided or otherwise licensed by Company pursuant to this Service Description.

- **COMPANY RECOMMENDS THAT CUSTOMER BACK UP ITS TECHNICAL AND PHYSICAL ENVIRONMENT, WHICH SHALL INCLUDE, WITHOUT LIMITATION: (A) SERVERS; (B) NETWORKS; (C) STORAGE; AND (D) PERFORM MAINTENANCE OF SUCH TECHNICAL AND PHYSICAL ENVIRONMENT BEFORE THE SERVICES START DATE. CUSTOMER ACKNOWLEDGES AND AGREES THAT SUCH BACK UP AND MAINTENANCE OF CUSTOMER'S TECHNICAL AND PHYSICAL ENVIRONMENT IS CUSTOMER'S SOLE RESPONSIBILITY AND COMPANY SHALL HAVE NO LIABILITY IN THIS REGARD WHATSOEVER.**

Third-Party Considerations

Third-Party Integration

Some Connectors provided in a Service may contain features designed to interoperate with other third-party tools, APIs, products, or services. As such, Company cannot guarantee the continued availability of such Service features should that third party cease to make interoperability available or in a commercially reasonable manner. Third party notices and third party flow-downs are available at https://www.arctera.com/license-agreements

Supported Platforms and Technical Requirements

The Service is compatible only with approved versions of on-premise mail servers and hosted mail services set forth in the current compatibility list at https://supportarctera.cloud.com/support-home/kbsearch/article?articleNumber=100040129.

Service-Specific Terms

Assistance and Technical Support

Customer Assistance: Company will provide the following assistance as part of the Service:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support: Company shall provide technical support services ("Support") to assist Customer with:

- Configuration and use of the Service;
- Diagnosis and resolution of incidents affecting the Service; and
- General technical inquiries related to the Service and any applicable software components.
- Support is provided in accordance with the support model described herein and any applicable Service Level commitments.

Support Model: Company provides Support based on the severity of the reported issue.

- Severity 1 (Critical) incidents are supported 22x5.
- Severity 2–4 issues are supported during applicable regional business hours.
- Weekend support for Severity 1 incidents is available Saturday and Sunday from 8:00 AM to 6:00 PM EST and is provided by on-call support personnel.

Severity levels will be determined jointly by Customer and Company based on the impact of the reported issue.

Maintenance: The Service is monitored on a twenty-four (24) hours/day by seven (7) days/week basis for hardware availability, service capacity, and network resource utilization. The Service is also regularly monitored for service level compliance and adjustments are made as needed. Company must perform maintenance on the Service Infrastructure in order to provide the Service in accordance with the Agreement. The following applies to such maintenance:

- **Planned Maintenance:** For Planned Maintenance, Company will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, or SMS or phone as requested. Company will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service. "**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

- **Emergency Maintenance:** Where Emergency Maintenance is necessary and is likely to affect the Service, Company will endeavor to inform the affected parties in advance via email, or SMS or by phone no less than one (1) hour prior to the start of the Emergency Maintenance. "**Emergency Maintenance**" means unscheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Company could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

Data Decommissioning

Customer Data will be decommissioned in the following events, or as otherwise set forth in this Service Description:

- Service cancellation (either by request of Customer or in the event of non-payment). For clarity, a notice of cancellation by Customer takes effect upon the expiration of the then-current Term and does not terminate the Service until the end of Customer's then-current term.
- Service termination or expiration.

Customer loses all access to the Service and its Customer Data immediately following suspension, expiration, or termination of the Service. If Customer needs a copy of their Customer Data, Customer must request a quote for such Customer Data prior to the Data Decommissioning event.

Decommissioned Customer Data will be deleted in accordance with Company's standard deletion practices within thirty (30) days of the Data Decommissioning event and is irretrievable thereafter.

Usage

Customer cannot reduce the agreed upon quantity during any pre-committed subscription term (“Minimum Commit”).

Additional Service Requirements

- Customer shall comply with all applicable laws with respect to use of the Service(s). In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service(s) is entirely in Customer’s control, therefore, Company is not liable for Customer’s use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

- The company reserves the right to update the Service at any time in order to maintain the effectiveness of the Service.

- The company reserves the right to modify usage measurement methodologies, classifications, or consumption weighting factors from time to time, provided such changes do not materially diminish the overall functionality of the subscribed services during the applicable subscription term.

- If Customer has not provided the requested provisioning information to allow Company to provide the Service, Company reserves the right to begin charging for the Service within thirty (30) days of receipt of an order for the Service.

- Customer Data shall be archived during the Term of the Service. Before the end of the Service term or upon termination of the Service, Customer shall make a written election for Company to: (i) delete Customer Data in accordance with the Data Decommissioning section; or (ii) Contracted renewal for Data Extraction/Export services at Company’s then current pricing (“Data Extraction”). In the event Customer fails to provide written instruction to Company as provided in the preceding sentence, Customer Data will be decommissioned in accordance with the Data Decommissioning section. Company reserves the right, in its sole discretion, to refuse any Data Extraction request until Customer’s account no longer has outstanding Services fees.

- Retention Periods. While Customer’s subscription is active, Customer Data is maintained according to the Customer-defined retention/expiry period, except where customer may opt in to WORM storage functionality with a 7-year retention period as specified at the time of order . Customer data is maintained for the duration of that retention period based on the mail date of the Customer Email. Thereafter, Customer Data will be deleted after the expiry of that retention period and will no longer be accessible at all. Regardless of the retention period purchased or set by Customer, all Customer Data is subject to deletion upon termination or expiration of the Services.

Service Level Agreement (“SLA”)

- Company’s Service Level Agreement shall provide 99.9% or higher Uptime for the Service.

- “Uptime” is defined as the time during which a Customer is able to Access the Service, as reported by the Service incident management system. “Access” is defined as a Customer being able to successfully login and use the Service functionality, as outlined in this Service Description.

- Uptime is measured every calendar month as a percentage value. The monthly Uptime percentage is the total number of minutes of Uptime achieved in a calendar month, divided by the total number of minutes in a calendar month.

Exclusions

- This SLA will not operate: (i) during periods of Planned Maintenance or Emergency Maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) due to overall internet congestion, slowdown or unavailability; (iii) bandwidth or other limitations caused by Customer internet service provider (ISP); (iv) unavailability of generic internet services (e.g. DNS servers); (v) a result of Customer equipment or third party computer hardware, software or network infrastructure not within the sole control of Company; (vi) during any period of suspension of service by Company in accordance with the terms of the Agreement; (vii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (viii) Customer has not configured the Service in accordance with the Agreement.

Service Credits

- If the Service does not meet the stated SLA, Customer may submit a Service Credit Request for a Service Credit. Service Credits are calculated as follows:

Availability	Service Credit[1]
≥=99.9%	0%
>=99.0% but <99.9%	10%
<99.0%	25%

[1] Service Credits are calculated as a percentage of the monthly cost of the service when the outage occurred (regardless of licensing model). Service Credit percentages in the table above are an aggregate maximum for all SLA claims for a single Service in a given calendar month. Service Credits only apply if the Customer’s account is current and not suspended for non-payment or other non-compliance with terms. Service Credits are provided to the party receiving the Company invoice.

- To successfully claim a Service Credit, Customer must submit a Service Credit Request within fifteen (15) business days of the end of the calendar month in which the suspected SLA non-compliance occurred. The request must specify which service was impacted, and the dates and times of service unavailability.

- Company will validate the information provided by the Customer and if a Service Credit is due, it will be applied against the next Company invoice for the Customer’s Service. If a Service Credit is successfully claimed for more than one Company Service, then the quantity will equal the number of credits applied and the total will be aggregated to reflect the total value of the Service Credits claimed in that measurement period.

- The remedies set out in this SLA shall be Customer’s sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this SLA.

Acceptable Use Policy

Company must preserve the integrity of the Service and maintain its Service commitments to all customers. Neither Customer, nor Customer’s Users, shall use the Service in a manner that negatively

impacts the security, integrity, or functionality of the Service or other customers' ability to use the Service, including, without limitation, the following activities:

- Use the Service for unlawful business purposes.
- Transmit, distribute, retrieve or store any data or other material through or via the Service that infringes, misappropriates, or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality, or viruses, trojan horses, worms, time bombs, cancel bots, or other computer programming routines that are intended to damage, detrimentally interfere with, intercept or expropriate any system, data, or Personal Data.
- Fraudulently conceal, forge, or otherwise falsify identities in connection with any use of the Service.
- Engage in any activities that may interfere with the ability of others to access or use the Service or the Internet (e.g., denial of service attacks).
- Monitor any data, information or communications on any network or system (including the Service) that Customer does not own or have authorization.
- Use the Service for benchmarking or competitive purposes or disclose the results of any test to a third party without Company's prior written consent.
- Use any method, such as a third-party tool, to perform or circumvent any of the functionality or restrictions of the Service. Company reserves the right to restrict such methodologies and tools from operating within its infrastructure.

Violation

If Customer becomes aware of any violation of this Acceptable Use Policy, Customer must notify Company as soon as reasonably practicable.

In the event of an emergency, Company may temporarily, and for a reasonable period only, suspend, block, or restrict access to information and network resources when it is reasonably necessary to do so to protect the integrity and security of the Service, without compensation to Customer of any kind. Company shall provide Customer advance notice of such suspension, if possible, and as soon as reasonably possible otherwise. To protect platform integrity, performance, and security, the use of automated tools, scripts, scraping technologies, or non-human interactions with the Service is prohibited unless explicitly approved in writing by the Company.