

## RUBRIK, INC. LICENSING GUIDE

<b>General Terms</b>	2
<b>Rubrik SaaS Application Protection Product Specific Terms</b>	4
Universal SaaS Application License	4
Rubrik for Microsoft Dynamics Data Protection	4
Rubrik for M365 Protection	5
Rubrik for Salesforce Data Protection	6
Rubrik for Jira Data Protection	7
Rubrik for Google Workspace Protection	8
<b>Rubrik Scale Program Terms</b>	10
Scale Subscription	11
Scale True Forward	11
<b>Rubrik Utility Program Terms</b>	13
Rubrik Security Cloud (RSC) Utility	13
<b>Rubrik Cloud Vault Product Specific Terms</b>	15
Rubrik Cloud Vault	15
Rubrik-hosted Universal Cloud License on RCV	17
Rubrik-hosted NAS Cloud Direct on RCV	18
<b>Rubrik Identity Recovery and Resilience</b>	19
<b>Rubrik Identity OKTA Recovery</b>	19
<b>Rubrik Artificial Intelligence Solutions</b>	20
<b>Rubrik Security Cloud – Government (“RSC-G”) Product Specific Terms</b>	22

## GENERAL TERMS

### Scope

The terms of this Rubrik Licensing Guide (“**Licensing Guide**”) are effective as of February 12, 2026 and supplement the Rubrik Service Agreement, Rubrik End User License Agreement, or equivalent agreement between Customer and Rubrik governing Customer’s use of the Rubrik Service (“**Agreement**”). All capitalized terms not defined herein are as defined in the applicable Agreement. This Licensing Guide includes these General Terms, as well as product specific terms for certain products incorporated herein.

### General Subscription Terms

Customer is eligible to upgrade to a higher service offering at any time during a Subscription Period. Customer may not downgrade to a lower service offering or quantity during an active Subscription Period. At the end of the Subscription Period, Customer may elect to downgrade at the time of renewal. The Subscription Period commences when the applicable Rubrik Service is made available to Customer.

### Dependent Add-Ons

Certain products and/or features cannot operate on a stand-alone basis and will only function as an add-on component to another pre-requisite Rubrik product (“**Dependent Add-On**”). Customer is therefore required to have the most current version of such pre-requisite Rubrik product with an active Support Services entitlement to use the Dependent Add-On. Customer may purchase Dependent Add-Ons that are not coterminous with Customer’s license for the pre-requisite product and may extend beyond the expiration of the license for the pre-requisite product (“**Extended Term**”).

In the event a Dependent Add-On is purchased for an Extended Term, but Customer does not renew the expired pre-requisite product license and Support Services entitlement, Customer may lose some or all functionality of the Dependent Add-On upon the expiration of the term of the pre-requisite product and Customer will not be entitled to a refund or credits for any portion of the remaining Dependent Add-On subscription.

### Recovery Licenses

Subject to availability, upon Customer request, Rubrik may make Recovery Licenses available for purchase. A “**Recovery License**” is a limited subscription license to be used solely for the purpose of recovering data backed up in Customer’s data centers prior to the termination or expiration of the applicable Rubrik Service. Recovery Licenses must be purchased within thirty (30) days of expiration or termination of the applicable Rubrik Service, do not include Support Services, migration assistance, or Professional Services, and are exclusive of any fees for data extraction as set forth elsewhere in this Licensing Guide. Recovery Licenses are not available for hosted offerings. Customer should contact its account team for details.

### Proactive Edition

Rubrik Proactive Edition includes user access analysis features which allow Customer to gain insights into which users in their organization have access to sensitive data and how they gained access to it. In order to enable these features, certain user access data, including user name, email, access group memberships, properties and type, will be extracted from Customer’s Active Directory backup. Customer may view user access information in both the dashboard and reports available via the Data Security Posture dashboard on the Rubrik Proactive edition user interface.

### Data Security

Certain Data Security products and features may utilize pre-defined policies and analyzers based on common data sets and formats to provide general suggestions for classifying data elements (“**Default Classifications**”). By using such products and features you understand and acknowledge that Default Classifications: (i) are not intended to be a comprehensive or exhaustive list of data elements and formats regulated by the GDPR, CCPA or any other applicable laws and regulations, and (ii) should not be solely relied upon to identify all data elements and formats of a certain type for any purpose, including legal or compliance.

### **Data Security Remediation**

Certain Data Security products and features enable Customers to apply labels, modify certain data elements, or otherwise remediate Customer Data (“**Data Security Remediations**”). By using such products and features, you understand and acknowledge that all Data Security Remediations are performed under Customer’s election and direction, and that Customer is solely responsible for ensuring the appropriateness and/or accuracy of all Data Security Remediations.

### **Professional Services**

Professional Services may be performed by Rubrik or subcontractors acting on Rubrik’s behalf for whom Rubrik is responsible in the same manner as its own employees. Rubrik warrants that: (i) it and its personnel have the necessary knowledge, skills, experience, qualifications and resources to perform the Professional Services; and (ii) the Professional Services will be performed in a professional and workmanlike manner in accordance with industry standards. Customer will provide: (a) good faith cooperation and access to such information, facilities, and equipment as reasonably required for Rubrik to provide the Professional Services; and (b) such assistance as reasonably requested from time to time. If, through no fault or delay by Customer, including Customer’s failure to comply with (a) and (b) above, the Professional Services do not conform to the foregoing warranty, and Customer notifies Rubrik within ten (10) days of Rubrik’s completion of the Professional Services, Rubrik will re-perform the non-conforming Professional Services at no additional cost to Customer. Unless otherwise agreed upon by the Parties in writing, Rubrik’s obligation to provide Professional Services to Customer expires on the earlier of: (i) completion of the Professional Services; or (ii) six (6) months from the date Rubrik accepts the Order for Professional Services. Credit for unused Professional Services is not transferable to any other services.

### **Authorized Service Providers**

Service providers must be authorized by Rubrik and execute an applicable Partner Agreement. Customer is responsible for any and all account access it grants to its service providers.

### **Sizing**

To the extent Rubrik participates in any sizing analysis, it is only for purposes of providing an estimate using information provided by Customer or a third party acting on Customer’s behalf. Rubrik does not validate the accuracy of any sizing-related information it receives. Customer is solely responsible for all sizing decisions and for any inaccuracies in any sizing analysis.



## RUBRIK SAAS APPLICATION PROTECTION PRODUCT SPECIFIC TERMS

### UNIVERSAL SAAS APPLICATION LICENSE

The Universal SaaS Application License (“**USL**”) is a single SKU available on a per-user basis that entitles a User to use one Rubrik SaaS Application Protection offering. A USL may be transferred between supported Rubrik SaaS Application Protection products (Rubrik for Microsoft Dynamics Protection, Rubrik for M365 Protection, Rubrik for Salesforce Protection, and Rubrik for Jira Protection). A USL supports up to 100GB of Data Protection Capacity per User. Rubrik defines “**Data Protection Capacity**” as all non-expired, downloaded data in the SLA Window, including relics, data churn, and the Exchange Archive Mailboxes that are protected by the Rubrik Service.

#### Overuse

Customer will refrain from any conduct that would, in Rubrik’s reasonable judgment, overload or adversely impact the Rubrik Service. Customer agrees it will not use the Rubrik Service to back up more User accounts than the quantity of Service Users it has purchased and it will not exceed the Data Protection Capacity supported per User.

#### Azure Usage Attribution

When Customer deploys the Rubrik Service, Microsoft can identify the installation of Rubrik Service with the deployed Azure resources. Microsoft can correlate these resources used to support the Rubrik Service. Microsoft collects this information to provide the best experiences with their products and to operate their business. The data is collected and governed by Microsoft’s privacy policies, located at <https://www.microsoft.com/trustcenter>.

#### Data Extraction Terms

While it is normal to restore and extract Customer Data from time-to-time to recover from data loss, there are product usage restrictions for the following data extraction purposes. Creating a secondary backup copy is not permitted with any Rubrik-hosted subscriptions. This includes creating frequent copies (either daily, weekly or monthly and anything in between) and exporting it to another location outside of the Rubrik Service. This is not an exhaustive list.

Customers based in the EU may extract a copy of their Rubrik-hosted backup data for post-termination purposes to the extent required by the EU Data Act (“**Extractable Data**”). For clarity, Extractable Data does not include Rubrik’s or Rubrik’s licensors’ intellectual property or trade secrets, or data that could compromise the integrity, security or availability of the Rubrik Service. If Customer requires a copy of Extractable Data in this situation, Customer must request a copy of their Extractable Data, and the backup of the Extractable Data must be completed prior to the expiration of the Subscription Period. Please note that Extractable Data will not be indexed at the other location the Customer chooses to store Extractable Data, and therefore Customer will not be able to browse through the Extractable Data or perform restores. More than 30 days may be required for the actual extraction and export of Extractable Data, depending on the Customer’s specific configuration, quantity of data, and other circumstances outside of Rubrik’s control. Rubrik will provide commercially reasonable assistance and information to aid in the extraction process, subject to the terms of the Agreement. Customer must pay any egress fees charged by third-party cloud service providers for data extraction. Customers should contact their account team for details.

### RUBRIK FOR MICROSOFT DYNAMICS DATA PROTECTION

These Rubrik for Microsoft Dynamics Data Protection (“**Rubrik Microsoft Dynamics Service**”) product specific terms explain core licensing concepts for the Rubrik Microsoft Dynamics Service.

#### Product Overview

Rubrik provides policy-based protection of Customers’ Microsoft Dynamics environment via its Rubrik Service platform. The solution enables security, simplicity and performance for backup and restore operations on Microsoft Dynamics platform data.

## Licensing Model and Definitions

The Rubrik Microsoft Dynamics Service is licensed on a per-user basis. Customer must purchase at least enough licenses to cover their entire licensed user base.

- A **“User”** for the Rubrik Microsoft Dynamics Service means the individual or individuals authorized by Customer to use Customer’s Microsoft Dynamics applications and whose Microsoft Dynamics data is backed up using the Rubrik Microsoft Dynamics Service.
- A User is considered managed if there exists at least one (1) restore point created in the past thirty-one (31) days. After a continuous month-period without backing up a given User, Customer will be able to apply that license to another User.
- Users are calculated for all Microsoft Dynamics applications as follows:
  - Unique users that are a part of an organization are licensed for Microsoft Dynamics 365.
  - Unique users that have full/direct access to one or more of the Microsoft Dynamics 365 applications are counted as unique users.
  - Note: Users with access to Dynamics only via a Dynamics Trial license are excluded from the count of unique users.

## Hosting

The Rubrik Microsoft Dynamics Service is offered in a Rubrik-hosted environment, in which all data and infrastructure is hosted in a Rubrik-managed public cloud environment. Upon configuration, Customer selects the geographic region for the Azure instance where Customer backup data will be stored. Customer acknowledges that the Rubrik Microsoft Dynamics Service enables the Customer to access Customer Data from any geographic location and permits the transfer or movement of Customer Data to various devices. Customer further acknowledges that use of the Rubrik Microsoft Dynamics Service involves processing of Customer Data outside of the Microsoft systems, including temporarily displaying Customer Data in the user interface of the Rubrik Microsoft Dynamics Service, to enable Customer to locate and restore Microsoft data.

## Renewals and Upgrades

The total User counts can be expanded at any point, which will be co-termed with the original Subscription Period. Subject to general availability, all Service Subscriptions are eligible for renewal at the end of the Subscription Period. Data extraction may be subject to a one-time fee.

## RUBRIK FOR M365 PROTECTION

These Rubrik for Microsoft 365 Protection (**“M365 Service”**) product specific terms explain core licensing concepts for the Rubrik for M365 Service.

### Product Overview

Rubrik provides policy-based protection of Customers’ Microsoft 365 application via its Rubrik Service platform. The solution enables security, simplicity and performance for search and restore operations across Exchange Online, OneDrive, SharePoint, and Teams.

### Licensing Model and Definitions

The Rubrik-hosted M365 Service is licensed on a combined per User and Data Protection Capacity basis.

For Example: A Customer with 1,000 Users and 5,000 GB of Data Protection Capacity must not exceed their usage on either User accounts protected with the Rubrik M365 Service or the Data Protection Capacity consumed with the Rubrik M365 Service. If the Customer exceeded either 1,000 users or 5,000GB of capacity, it would be out of compliance.

A **“User”** of the M365 Service means the individual or individuals authorized by Customer to use Customer’s Microsoft 365 applications and whose Microsoft 365 data is backed up using M365 Service. For clarity, a User includes non-person mailboxes such as a shared



calendar. A User is considered managed if there exists at least one (1) restore point created in the past thirty-one (31) days. After a continuous month-period without backing up a given User, Customer will be able to apply that license to another User. The count of Users is the greater of the number of user mailboxes, the number of shared mailboxes, and the number of OneDrives that are protected using the M365 Services.

**“Data Protection Capacity”** means all non-expired downloaded Customer Data in the SLA window, including relics, data churn, and the Exchange Archive Mailboxes that are protected by the Rubrik Service.

Capacity usage on Microsoft’s reports is a point-in-time measurement that does not include relics, data churn, and the Exchange Archive Mailboxes that are protected in the M365 Service (and thus included in Rubrik’s capacity count). Because of this difference, Rubrik’s capacity reports may show higher capacity usage than native M365 reports.

### **Hosting Options: Rubrik-Hosted or Customer-Hosted**

By default, the M365 Service is offered in a Rubrik-hosted environment, in which all data and infrastructure is hosted in a Rubrik-managed public cloud environment. Upon configuration, Customer selects the geographic region for the Azure instance where Customer backup data will be stored. The M365 Service also supports a multi-geo option. However, a Customer-hosted option is available for customers who wish to manage their own data and infrastructure. Customer acknowledges that the M365 Service enables the Customer to access Customer Data from any geographic location and permits the transfer or movement of Customer Data to various devices.

### **Renewals and Upgrades**

The total User count and Data Protection Capacity can be upgraded at any point, which will be co-termed with the original Subscription Period. Customer is likewise allowed to transition from Customer-hosted to Rubrik-hosted offerings and standalone to bundle offerings at any time. Any such transition will require a placement of an Order and may incur an additional fee.

Subject to general availability, all M365 Service Subscriptions are eligible for renewal at the end of the Subscription Period. Data extraction may be subject to a one-time fee.

### **Trials**

Free Trials of the Rubrik-hosted M365 Service are limited to no more than five hundred (500) Users and 10TB of Data Protection Capacity.

## **RUBRIK FOR SALESFORCE DATA PROTECTION**

These Rubrik for Salesforce Data Protection (**“Rubrik Salesforce Service”**) product specific terms explain core licensing concepts for the Rubrik Salesforce Service.

### **Product Overview**

Rubrik provides policy-based protection of Customers’ Salesforce environment via its Rubrik Service platform. The solution enables security, simplicity and performance for backup and restore operations on Salesforce platform data.

### **Licensing Model and Definitions**

The Rubrik Salesforce Service is licensed on a per-user basis. Customers must purchase at least enough licenses to cover their licensed user base for their Salesforce production environment, where the licensed user base is equal to the sum of active “Salesforce” and “Salesforce Platform” user licenses of the Salesforce production environment protected. Customers can associate one (1) Full Sandbox and unlimited Developer, Developer Pro, and Partial Copy Sandboxes for each production environment protected. Customers can refer to the Salesforce license usage in their Salesforce Admin Console to find the number of users.

A **“User”** for the Rubrik Salesforce Service means the individual or individuals authorized by Customer to use Customer’s Salesforce environment of the Salesforce Org that is backed up using the Rubrik Salesforce Service.

Rubrik counts the total number of active Salesforce and Salesforce Platform user licenses each day. The license usage amount may vary each day depending on Salesforce user usage. If Customer's Salesforce usage amount for the applicable Salesforce Org decreases, the remaining number of licensed Users can be applied to another of Customer's Salesforce Orgs.

### **Hosting**

The Rubrik Salesforce Service is offered in a Rubrik-hosted environment, in which all data and infrastructure is hosted in a Rubrik-managed public cloud environment. Upon configuration, Customer selects the geographic region for the Azure instance where Customer back-up data will be stored. Customer acknowledges that the Rubrik Salesforce Service enables the Customer to access Customer Data from any geographic location and permits the transfer or movement of Customer Data to various devices. Customer further acknowledges that use of the Rubrik Salesforce Service involves transmitting and processing of Customer Data outside of the Salesforce systems, including temporarily displaying Customer Data in the user interface of the Rubrik Salesforce Service, to enable Customer to efficiently locate and restore selected Salesforce data. Customer back-up data will be securely stored and protected by Rubrik outside of Salesforce's system rather than subject to protection by Salesforce.

### **Porting Data to Sandbox or Test/Dev Environments**

Customer must have an active entitlement to Salesforce DevOps to be permitted to port or seed Customer Data backed up using the Rubrik Salesforce Service into a sandbox org for test/dev purposes. If Customer does not have such entitlement, then Customer must use the Rubrik Salesforce Service only for backup and recovery.

### **Renewals and Upgrades**

The total User counts can be expanded at any point, which will be co-termed with the original Subscription Period. Subject to general availability, all Service Subscriptions are eligible for renewal at the end of the Subscription Period. Data extraction may be subject to a one-time fee.

## **RUBRIK FOR JIRA DATA PROTECTION**

These Rubrik for Jira Data Protection ("**Rubrik Jira Service**") product specific terms explain core licensing concepts for the Rubrik Jira Service.

### **Product Overview**

Rubrik provides policy-based protection of Customers' Jira software environment via its Rubrik Service platform. The solution enables security, simplicity and performance for backup and restore operations on Jira software data.

### **Licensing Model and Definitions**

The Rubrik Jira Service is licensed on a per-user basis. Customer must purchase at least enough licenses to cover their entire licensed user base. Customers can refer to their Jira software license usage in their Jira Admin Console to easily find the count.

A "**User**" for the Rubrik Jira Service means the individual or individuals authorized by Customer to use Customer's Jira Software environment of the site(s) that are protected using the Rubrik Jira Service.

Rubrik counts the total number of active users with assigned Jira Software licenses that have access to the site being protected. The Rubrik Jira Service can protect multiple sites, so if the Customer has multiple sites to protect, the product will count the number of users for each site.

## Hosting

The Rubrik Jira Service is offered in a Rubrik-hosted environment, in which all data and infrastructure is hosted in a Rubrik-managed public cloud environment. Upon configuration, Customer selects the geographic region for the Azure instance where Customer backup data will be stored. Customer acknowledges that the Rubrik Jira Service enables the Customer to access Customer Data from any geographic location and permits the transfer or movement of Customer Data to various devices.

## Renewals and Upgrades

The total User counts can be expanded at any point, which will be co-termed with the original Subscription Period. Subject to general availability, all Service Subscriptions are eligible for renewal at the end of the Subscription Period. Data extraction may be subject to a one-time fee.

## RUBRIK FOR GOOGLE WORKSPACE PROTECTION

These Rubrik for Google Workspace Protection (“**GWS Service**”) product specific terms explain core licensing concepts for the Rubrik for GWS Service.

### Product Overview

Rubrik provides policy-based protection of Customers’ Google Workspace application via its Rubrik Service platform. The solution enables security, simplicity and performance for search and restore operations across Gmail and GDrive.

### Licensing Model and Definitions

The Rubrik-hosted GWS Service is licensed on a combined per User and Data Protection Capacity basis.

For Example: A Customer with 1,000 Users and 5,000 GB of Data Protection Capacity must not exceed their usage on either User accounts protected with the Rubrik GWS Service or the Data Protection Capacity consumed with the Rubrik GWS Service. If the Customer exceeded either 1,000 users or 5,000GB of capacity, it would be out of compliance.

A “**User**” of the GWS Service means the individual or individuals authorized by Customer to use Customer’s GWS applications and whose GWS data is backed up using GWS Service. A User is considered managed if there exists at least one (1) restore point created in the past thirty-one (31) days. After a continuous month-period without backing up a given User, Customer will be able to apply that license to another User. The count of Users is the unique count of users across user mailboxes and GDrives that are protected using the GWS Services.

For Example: A Customer with 200 unique users on Gmail and GDrive both, and another 100 unique users on GDrive only will need 300 user licenses to protect all users.

“**Data Protection Capacity**” means all non-expired downloaded Customer Data in the SLA window, including relics, and data churn that are protected by the Rubrik Service. Capacity usage on Google’s reports is a point-in-time measurement that does not include relics, data churn, that are protected in the GWS Service (and thus included in Rubrik’s capacity count). Because of this difference, Rubrik’s capacity reports may show higher capacity usage than native GWS reports.

### Hosting Options: Rubrik-Hosted

By default, the GWS Service is offered in a Rubrik-hosted environment, in which all data and infrastructure is hosted in a Rubrik-managed public cloud environment. Upon configuration, Customer selects the geographic region for the GCP instance where Customer backup data will be stored. The GWS Service also supports a multi-geo option. Customer acknowledges that the GWS Service enables the Customer to access Customer Data from any geographic location and permits the transfer or movement of Customer Data to various devices.

**Renewals and Upgrades**

The total User count and Data Protection Capacity can be upgraded at any point, which will be co-termed with the original Subscription Period. Subject to general availability, all GWS Service Subscriptions are eligible for renewal at the end of the Subscription Period.

**Trials**

Free Trials of the Rubrik-hosted GWS Service are limited to no more than ten (10) Users and 500GB of Data Protection Capacity.



## RUBRIK SCALE PROGRAM TERMS

These Rubrik Scale program license terms include core licensing concepts for the Rubrik Scale Subscription, True-Forward, and Utility offerings.

### GENERAL TERMS

#### Program Overview

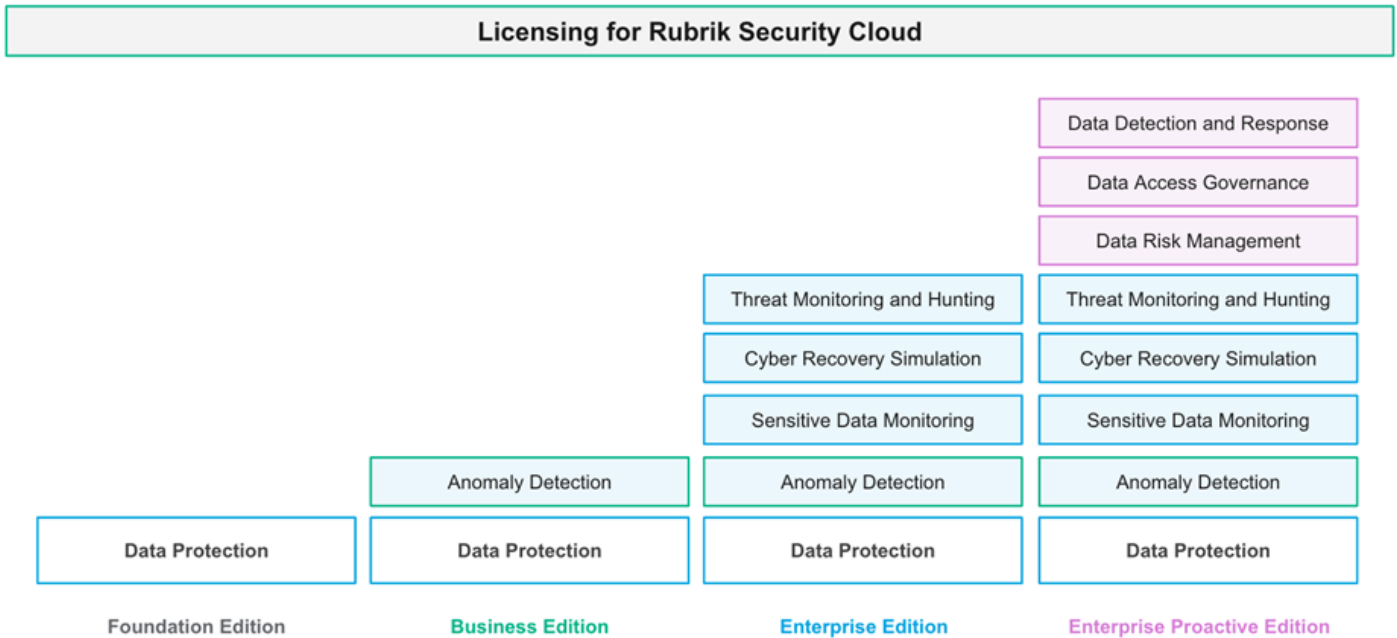
Rubrik Scale is available in two (2) licensing models: (1) the Scale Subscription model, which allows Customer license portability between Rubrik appliances, third-party appliances and cloud platforms; and allows Customer to purchase different quantities of hardware and software capacity; and (2) the Scale True Forward model, which, in addition to the attributes of Scale Subscription, allows Customer to purchase additional capacity via “True Forward Cycles”.

- “Back-end Terabyte” (“**BETB**”) means: The final volume of data protected after compression, deduplication, replication, or other data operations, regardless of the storage target.
- “Front-end Terabyte” (“**FETB**”) means: The initial volume of primary data submitted to Rubrik, before compression, deduplication, replication, or other data operations.

#### Packaging Overview

Both Scale models are licensed as three-year subscriptions with the option to extend to five (5) years. With a single license, Customer can deploy and scale across all hardware and cloud platforms.

Below are the four (4) different packages offered with each Scale model:



Note: When one (1) TB is purchased, Customer is only entitled to one (1) TB on one (1) of the following platforms: RSC, Edge, or Universal Cloud License, not one (1) TB on each of those platforms. By default, Scale Subscription and Scale True Forward on-premise workloads are measured on a BETB basis, and cloud workloads are measured on a FETB basis. FETB measurements for on-premise workloads may be available, subject to approval.

If and when Customer chooses to migrate that one (1) TB of RSC to the cloud, that one (1) TB on-prem will convert to one (1) TB of Universal Cloud License. If Customer requires additional Universal Cloud licensing in addition to the converted licenses, Customer must purchase additional quantities of the license.

### **Hardware Purchase Policy**

Hardware purchase policies differ between the Scale models, as noted for each Scale model. For avoidance of doubt, e1000 appliances may not be purchased as part of any Scale model offering.

Scale Orders may be placed for use on third-party hardware. Rubrik-branded hardware must be purchased upfront if it is required for a Rubrik Scale purchase. Rubrik-branded hardware may not be purchased during the Subscription Period of an applicable Scale Order which was originally placed for use with third-party hardware.

### **License Portability**

Customer may migrate its Scale licenses across any Rubrik-approved platform(s), including Rubrik-branded hardware, third-party hardware and the public cloud anytime during the applicable Subscription Period without the need to purchase additional Scale licenses (subject to the Customer's licensed capacity). If Customer wishes to migrate data to or from a Rubrik-approved public cloud platform, Customer may convert existing Scale licenses for on-premise storage to Universal Cloud License (1 BETB = 1 FETB), or vice versa.

Rubrik can provide Professional Services to assist Customer to migrate data across hardware platforms upon Customer's placement of an Order for such Professional Services.

## **SCALE SUBSCRIPTION MODEL TERMS**

Includes all of the General Terms listed above for Scale purchases.

- **Licensing.** Scale Subscription allows Customer license portability between Rubrik-branded hardware, third-party hardware, and cloud platforms, and allows Customer to purchase greater SaaS capacity than hardware capacity.
- **Customer Experience Manager (CEM) Requirement.** A CEM may be required for certain Scale Subscription Orders. Customer should confirm applicability with its Reseller.
- **Renewals.** Scale Subscription licenses may be renewed for a minimum of twelve (12) and a maximum of sixty (60) months.

## **SCALE TRUE FORWARD MODEL TERMS**

Includes all of the General Terms listed above for Scale purchases.

- **Licensing.** In addition to the license portability of the Scale Subscription license, Scale True Forward allows Customer to purchase different quantities of hardware and SaaS capacity, as described below, and allows Customer to exceed capacity and to purchase additional capacity via "**True Forward Cycles**," as described below. The initial Scale True-Forward Subscription Period must be for a minimum of thirty-six (36) months. Scale True Forward is available on an approval basis only.
- **CEM Requirement.** A CEM is required to be purchased for all Scale True Forward Orders.
- **Renewals.** Scale True Forward licenses may be renewed for a minimum of thirty-six (36) and a maximum of sixty (60) months.
- **Scale True Forward Hardware Policy.** At time of purchase and throughout the Subscription Period of the Scale True Forward license, Rubrik permits thirty percent (30%) more SaaS capacity than hardware capacity. This thirty percent (30%) capacity difference only applies to Rubrik-branded hardware purchases, not third-party hardware purchases.

- **Scale True Forward Model Capacity Purchases.** During the Scale True-forward Subscription Period, the CEM will help Customer plan capacity through monthly usage reporting via SentryAI. Customer can add more capacity during any Subscription Period (co-termed to the end of the Subscription Period), based on actual usage. Rubrik will not retroactively charge for unplanned capacity consumed before each Scale Review.
- **True Forward Scale Reviews.** During the Scale True Forward Subscription Period, Rubrik will conduct semi-annual reviews of usage data logs for Customer's global environment to determine the utilized TB capacity ("**Scale Review**"). The first Scale Review will occur approximately six (6) months from the date of the Scale True Forward Order and then once every six (6) months thereafter during the Scale True-Forward Subscription Period.

If the results of a Scale Review indicate Customer's total utilized capacity exceeds the Scale True Forward capacity purchased, then Rubrik will issue a quote to the applicable channel partner for additional capacity greater than or equal to the seventy-fifth percentile of daily peak usage in the 6-month Scale Review period (or minimum capacity hardware, whichever is larger). Customer agrees to place an Order with its Reseller for such additional Scale True Forward capacity within thirty (30) days of receipt of its Reseller's quote.

- **Capacity Burst Events.** In addition to the semi-annual Scale Reviews, if daily usage data shows that the utilized capacity exceeds the total Scale True Forward capacity purchased by more than thirty percent (30%) at any time prior to the next Scale Review (a "**Capacity Burst**"), then Rubrik will issue a quote to the applicable channel partner for additional capacity greater than or equal to the seventy-fifth percentile of daily peak usage in the current Scale Review period. Customer agrees to place an Order with its Reseller for such additional Scale True Forward capacity within thirty (30) days of receipt of its Reseller's quote. Capacity Burst purchases will be prorated from the date of the Capacity Burst to the end of the Scale True Forward Subscription Period. The next Scale Review will still occur, as described above.

## RUBRIK UTILITY PROGRAM TERMS

### UTILITY MODEL TERMS

The Utility model offers a consumption billing model with flexibility for on-demand capacity. Utility Model purchases are capacity-based licenses (either terabyte or user-based) which flex to permit additional capacity on demand.

### RUBRIK SECURITY CLOUD (RSC) UTILITY (FOR BUSINESS AND ENTERPRISE EDITIONS)

- **Licensing.** The Utility model offers a consumption billing model with flexibility for On-Demand Capacity. The initial Utility Subscription Period must be for a minimum of thirty-six (36) months. Utility licenses are subject to a Reserve Capacity commitment, plus On-Demand Capacity, if any, as described below.
- **CEM Requirement.** A CEM may be required for certain Utility Orders. Customer should confirm applicability with its Reseller.
- **Definitions:**
  - **“Reserve Capacity”** means the minimum committed capacity [number of Terabytes (TBs)] purchased by Customer as set forth in the applicable Order.
  - **“On-Demand Capacity”** means the actual capacity used above the Reserve Capacity.
  - **“Total Usage”** means Reserve Capacity plus On-Demand Capacity, if any.
  - **“Billing Report”** means the report run on the 25th of each month of the Utility Subscription Period showing Total Usage.
  - **“Customer”** means as applicable the end user or the service delivery partner (SDP).
  - **“Reseller”** means the Reseller (where Customer is the end user) or the distributor (where Customer is a SDP).
- **Measurement.** Utility Total Usage is measured on a per Terabyte (TB) or per user basis using the metering metric, as indicated in the applicable Order, and as indicated in the Billing Report. The applicable metering metric must remain constant for the duration of the Subscription Period and any renewal. Customer may be required to assist Rubrik in verifying the accuracy of Total Usage for Billing Report purposes.
- **Reserve Capacity and On-Demand Capacity.**
  - Reserve Capacity for the Utility Subscription Period will be invoiced in advance for the billing period by the applicable channel partner at the time the Utility Order is placed.
  - If a Billing Report indicates Customer’s Total Usage exceeds the Reserve Capacity, then Rubrik will issue an invoice to the applicable channel partner for the On-Demand Capacity. Customer agrees to pay its Reseller for such On-Demand Capacity as set forth in the Order.
- **Requirements & Terms by product:**
  - **RSC:**
    - RSC Utility clusters shall not be mixed or used with any other cluster (e.g., RSC Utility and standard Rubrik Security Cloud, or any previously licensed RCDM cluster cannot be in the same cluster).

- All clusters must remain with the originally assigned RSC Utility purchase (Foundation or Enterprise Edition). Additional RSC Utility purchases may not be added to the cluster(s) associated with any previous RSC Utility purchase.
  - Customer must assist Rubrik in linking cluster IDs to the applicable RSC Utility Order.
  - RSC Utility FETB and BETB models cannot be combined.
- **M365:**
    - M365 user and data protection capacity licenses must not be combined with the Universal SaaS license under the Utility program for M365 coverage. Customers must select either the M365 user and data protection capacity licenses or the Universal SaaS license to cover M365 protection. Although customers can purchase both license types, the Universal SaaS license cannot be applied to M365 protection and is limited to other non-M365 SaaS applications.



## RUBRIK CLOUD VAULT PRODUCT SPECIFIC TERMS

These Rubrik Cloud Vault (“RCV”) product specific terms explain core licensing concepts for RCV. Additional product specific terms applicable to Rubrik-hosted Universal Cloud License and Rubrik-hosted NAS Cloud Direct are included below in this Section. All General RCV Terms are applicable to Subscriptions for Rubrik-hosted Universal Cloud License and Rubrik-hosted NAS Cloud Direct.

### GENERAL RCV TERMS

#### Product Overview

RCV is a cloud storage service for Customer back-up data hosted in a Rubrik-managed instance of Azure, AWS or GCP.

#### Procurement Options

RCV is available as an add-on product to the Rubrik Service. Customer is required to have a Rubrik Security Cloud subscription as a prerequisite to use RCV. RCV licenses are offered on a per back-end terabyte pricing model. Pricing varies depending on the storage tier or redundancy zone selected, as such options are further described in the Data Storage and Redundancy section below.

#### Renewals and Upgrades

License tiers and total license counts can be upgraded at any point, co-termed with the original Subscription Period. Subject to general availability, all RCV licenses are eligible for renewal at the end of the Subscription Period. Data extraction may be subject to a one-time fee.

#### Data Storage and Redundancy

There are two (2) RCV storage tiers available for purchase—backup and archive, as well as up to three (3) redundancy options—single zone, multi zone, and multi region redundancy. Single zone redundancy means the data is stored in a single geographic location within a region. Multi zone redundancy means the data is replicated automatically across multiple locations within a region. Multi region redundancy means the data is replicated automatically to another region paired with the selected primary region. Customers may purchase a mix of storage tiers and redundancy options based on their need, subject to availability on the selected cloud storage platform.

The license cost varies depending on the selected combination of storage tier and redundancy options. Customers pay for their storage upfront subject to a minimum one (1)-year Subscription Period. Customer commits to one or more storage tiers upfront and buys capacity related to that specific tier and redundancy. Customers may not switch storage amounts between tiers and redundancies.

Customer is responsible for selecting the geographic region of the instance storing Customer back-up data. Customer acknowledges that RCV enables Customer to access Customer Data from any geographic location and enables Customer to transfer or move Customer Data to various Customer devices.

The table below illustrates the RCV storage and redundancy configurations currently available for each supported cloud platform.

Redundancy Option	Storage Tier	Platforms Available		
		Azure	AWS	GCP
Single Zone	Backup Tier	✓	✓	

	Archive Tier	✓		
Multi Zone	Backup Tier	✓	✓	✓
	Archive Tier		✓	✓
Multi Region	Backup Tier	✓		

### Capacity Entitlement

RCV usage is measured in BETB corresponding to the data stored in RCV. The usage (BETB) is compared with the capacity purchased under the applicable Order (“**Capacity Entitlement**”) continuously to evaluate if usage has exceeded the Capacity Entitlement. Usage is aggregated for comparison separately for each RCV SKU configuration. Customer will not use RCV to store more terabytes of Customer Data than the Capacity Entitlement, and it is solely Customer’s obligation to not exceed the Capacity Entitlement. Customer acknowledges and agrees that Customer Data exceeding the Capacity Entitlement will not be stored on RCV.

### Egress Limits

Customer will not download more than ten percent (10%) of its total Customer Data from RCV during each twelve (12) months of the applicable Subscription Period (“**Egress Limit**”). The foregoing Egress Limit will not apply in the event Customer is responding to: (a) a cybersecurity incident, where a “cybersecurity incident” is the occurrence of an event that prompts an organization to require a response and recovery because the event either (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of applicable cybersecurity and privacy laws or regulations; or, (b) a force majeure or disaster recovery event which results in the originating infrastructure being inaccessible for recovery efforts.

### Minimum Storage Period

Customer must adhere to the following minimum storage periods for Customer Data, according to the specific tier purchased: (a) for the Azure storage tier designated for backup, Customer Data must remain stored on RCV for a minimum of thirty (30) consecutive days from the date initially stored; (b) for the Azure storage tier designated for archive, Customer Data must be stored on RCV for a minimum of one hundred and eighty (180) consecutive days.

### Usage Attribution

When Customer deploys RCV on Azure, AWS or GCP, the respective cloud platform provider (i.e., Microsoft or AWS) can identify and correlate the Rubrik Service installation that is using the Azure or AWS resources and attribute the amount of such resources used to support the Rubrik Service. The cloud platform providers collect this information to provide the best experiences with their products and to operate their business, in accordance with their respective privacy policies located at <https://www.microsoft.com/trustcenter> (Microsoft) and <https://aws.amazon.com/privacy/> (AWS).

### Data Extraction Terms

While it is normal to restore and extract data from time-to-time to recover from data loss, there are product usage restrictions for the following data extraction purposes. Creating a secondary backup copy is not permitted with any Rubrik-hosted subscriptions. This includes creating frequent copies (either daily, weekly or monthly and anything in between) and exporting it to another location outside of the Rubrik Service. This is not an exhaustive list.

Customers based in the EU may extract a copy of their Rubrik-hosted backup data for post-termination purposes to the extent required by the EU Data Act (“**Extractable Data**”). For clarity, Extractable Data does not include Rubrik’s or Rubrik’s licensors’ intellectual property or trade secrets, or data that could compromise the integrity, security or availability of the Rubrik Service. If Customer requires a copy of Extractable Data in this situation, Customer must request a copy of their Extractable Data, and the backup of the Extractable Data must be completed prior to the expiration of the Subscription Period. Please note that Extractable Data will not be indexed at the other location the Customer chooses to store Extractable Data, and therefore Customer will not be able to browse through the Extractable Data or perform restores. More than 30 days may be required for the actual extraction and export of Extractable Data, depending on the Customer’s specific configuration, quantity of data, and other circumstances outside of Rubrik’s control. Rubrik will provide commercially reasonable assistance and information to aid in the extraction process, subject to the terms of the Agreement. Customer must pay any egress fees charged by third-party cloud service providers for data extraction. Customers should contact their account team for details.

## **RUBRIK-HOSTED UNIVERSAL CLOUD LICENSE ON RCV**

The following product specific terms apply to the Universal Cloud License (“**UCL**”). UCL is offered by Rubrik as either Customer-hosted or hosted by Rubrik on RCV (“**Rubrik-hosted UCL**”). Customer consents to Customer Data storage in Rubrik RCV for Rubrik-hosted UCL.

### **Product Overview**

UCL includes Rubrik’s Cloud Native Protection and Cloud Cluster-ES products.

### **Capacity Entitlement**

UCL is offered on a FETB pricing model. FETB corresponds to the initial volume of primary data submitted to Rubrik, before compression, deduplication, replication, or other data operations. This definition of ‘FETB’ represents the capacity of data stored or utilized on a cloud workload. Actual UCL usage is compared with the capacity purchased under the applicable Order (“**Capacity Entitlement**”) continuously to evaluate if usage has exceeded the Capacity Entitlement.

### **Procurement Options**

Rubrik-hosted UCL uses RCV as a data storage target and offers additional data security features. Rubrik-hosted UCL requires the purchase of Rubrik Cloud Vault. To use certain Rubrik security features with UCL, Customer must purchase the specific UCL bundle containing those features.

Note: One (1) TB of Rubrik Security Cloud entitles the Customer to only one (1) TB on one (1) of the following platforms: Rubrik Security Cloud, Edge, or Universal Cloud License-Foundation Edition. If Customer migrates one (1) TB of Rubrik Security Cloud on-premise to the cloud, that one (1) BETB on-premise converts to one (1) FETB of Universal Cloud License- Foundation Edition. Any additional Universal Cloud licensing (capacity and/or functionality beyond UCL- Foundation Edition), must be purchased.

### **Configuration**

Customer Data protected using Rubrik-hosted UCL is stored in a RCV backup tier. Customer back-up data in RCV is hosted in the same Azure geographic region as the source data.

### **Minimum Storage Period**

Customer Data stored using Rubrik-hosted UCL must remain stored on RCV for a minimum of thirty (30) consecutive days from the date initially stored.

### **Overuse**

Customer will not engage in any conduct that would, in Rubrik’s reasonable judgment, overload or adversely impact the Rubrik Service, including RCV.

## RUBRIK-HOSTED NAS CLOUD DIRECT ON RCV

The following product specific terms apply to NAS Cloud Direct (“**NAS CD**”). NAS CD is offered by Rubrik as either Customer-hosted or hosted by Rubrik on RCV (“**Rubrik-hosted NAS CD**”). For Rubrik-hosted NAS-CD, Customer consents to Customer back-up data storage in Rubrik’s RCV Service.

### Product Overview

NAS CD enables Customer to secure file data stored on NAS devices accessible via SMB and NFS file storage protocols. NAS CD secures the data by backing up the files from NAS devices to a variety of storage targets including on premise/cloud based NFS or S3 compatible storage targets.

### Capacity Entitlement

NAS-CD is offered on a FETB pricing model. FETB corresponds to the initial volume of primary data submitted to Rubrik, before compression, deduplication, replication, or other data operations. Actual NAS-CD usage is compared with the capacity purchased under the applicable Order (“**Capacity Entitlement**”) continuously to evaluate if usage has exceeded the Capacity Entitlement.

### Procurement Options

Rubrik-hosted NAS CD uses RCV as a data storage target and offers additional data security features. Rubrik-hosted NAS CD requires the purchase of Rubrik Cloud Vault. To use certain Rubrik security features with NAS CD, Customer must purchase the specific NAS CD bundle containing those features.

### Configuration

Customer back-up data protected using Rubrik-hosted NAS CD is stored in a RCV archive tier and must be hosted in a geographic region where RCV is available. Customer back-up data in RCV is hosted in the same Azure geographic region as the source data.

### Overuse

Customer will not engage in any conduct that would, in Rubrik’s reasonable judgment, overload or adversely impact the Rubrik Service, including RCV.

## RUBRIK IDENTITY RECOVERY AND IDENTITY RESILIENCE

### Product Overview

Identity Recovery includes capabilities to recover a clean copy of Customer's Microsoft Active Directory (“AD”) or Entra ID environment.

Identity Resilience includes capabilities which proactively identify risks and monitor for indicators of compromise of identities in Customers' AD or Entra ID environment and allows the Customer to recover a clean copy of AD or Entra ID.

### Licensing Model and Definitions

Identity Recovery and Identity Resilience are licensed on a per-user basis. Customers must purchase licenses for their entire licensed user base, where the 'licensed user base' equals the greater of the number of enabled user accounts in all AD domains or in all EntraID tenants managed by the Rubrik Service (whichever is higher). A domain or tenant is managed by the Rubrik Service if it has been configured for backups within the Rubrik Service. Other AD objects such as groups, computers, and/or roles are not included in the user counts.

### Renewals and Upgrades

During a Subscription Period, Customers may purchase additional licensed users, which will be co-termed with the original Subscription Period. Subject to general availability, Identity Recovery and Identity Resilience Subscriptions are eligible for renewal at the end of a Subscription Period.

## RUBRIK IDENTITY OKTA RECOVERY

### Product Overview

Identity Okta Recovery includes capabilities to recover a clean copy of Customer's Okta environment.

### Licensing Model and Definitions

Identity Okta Recovery is licensed on a per-user basis. Customers must purchase licenses for their entire licensed user base, where the 'licensed user base' equals number of enabled user accounts Okta tenants managed by the Rubrik Service. A domain or tenant is managed by the Rubrik Service if it has been configured for backups within the Rubrik Service. Other objects such as groups, computers, and/or roles are not included in the user counts.

### Renewals and Upgrades

During a Subscription Period, Customers may purchase additional licensed users, which will be co-termed with the original Subscription Period. Subject to general availability, Identity Okta Recovery is eligible for renewal at the end of a Subscription Period.

## RUBRIK ARTIFICIAL INTELLIGENCE SOLUTIONS PRODUCT SPECIFIC TERMS

### Definitions

- **“AI”** means artificial intelligence that generates new content such as text, images and sounds.
- **“AI Solution(s)”** means a standalone Rubrik Service and/or components of the Rubrik Service that incorporate AI, as specified in the Documentation.
- **“Input”** means a natural language query or prompt that Customer submits to an AI Solution.
- **“Output”** means a response generated by an AI Solution and provided to Customer in response to an Input.
- **“Model”** means a pre-trained, third party large language model included in an AI Solution. For clarity, Models are Non-Rubrik Applications.

Rubrik offers certain AI Solutions that Customers may use to manage AI operations and respond to cyberattacks and operational failures in its environments.

### RUBY

Ruby is an AI-powered chatbot available as an optional feature in Rubrik Security Cloud (RSC) that can assist Customers with threat investigations within the Rubrik Service by answering questions, suggesting next steps, and facilitating execution of specific tasks. The use of Ruby is optional and is not enabled by default. To activate Ruby, Customer’s designated administrative user must opt in via a checkbox in the RSC user interface linking to these terms and conditions. Ruby utilizes Microsoft Azure OpenAI, which resides in Rubrik’s Azure instance, to understand user intent and generate natural language responses.

### ANNAPURNA

Annapurna is a generative AI-powered tool that enables Customer to query its Customer Data. Annapurna is a separately purchased product subject to a separate service agreement and is not made available by default in Rubrik Security Cloud.

### RUBRIK AGENT CLOUD (“RAC”)

- Product Overview: RAC is a standalone agent operations platform designed to provide Customer with tools to monitor AI agent actions on its data, provide guardrails on those actions, find the root causes of actions, and help Customer remediate the actions to repair changes to data and configurations. RAC utilizes pre-trained LLMs from Microsoft Azure OpenAI Service as well as pre-trained open source or otherwise publicly available models.
- Hosting Options: As the product develops, RAC may offer different hosting options. Specific hosting modalities are as set forth in the applicable Reseller quote.
- Licensing: RAC is licensed on a platform fee basis for a standard term of twelve (12) months. Use is permitted up to the fair use limits set forth in the applicable Reseller quote.

The Service Level Agreement is not applicable to AI Solutions. Notwithstanding anything to the contrary in the Agreement, Downtime that results from a failure of a third-party service in an AI Solution is not included in Service Commitment and Downtime calculations. Chat transcripts produced by AI Solutions (which may include Customer information) are stored in Customer’s tenant-specific database in RSC until deleted by Customer. Subject to Rubrik’s ownership of the Rubrik Service, Documentation, Support Services and Professional Services, Customer Inputs and Outputs to AI Solutions are Customer Data. Customer Data will not be used to train or fine-tune Models without Customer’s consent. Customer acknowledges that, due to the nature of AI and the technology powering the AI Solutions, Output may not be unique, and Customer acknowledges that Rubrik or others may generate the same or substantially similar output. Output may be inaccurate, incomplete, or reflect errors, biases, or other limitations due to the contents of Input. Customer is solely responsible for: (i) reviewing all Output and verifying its accuracy and legality before use; (ii) developing and enforcing internal policies regarding appropriate use of AI Solutions and training authorized users accordingly; (iii) providing all notices and obtaining all consents required by applicable law; and (iv) implementing sufficient human oversight for Customer’s use of the AI Solutions. Customer assumes sole risk for its use of any Output. The AI Solutions are not intended for any use case involving biometrics, health information, safety components in critical infrastructure, or other high-risk processing activities. Certain Models



may be subject to different or additional terms, which will be made reasonably available to Customer via the AI Principles at: [Customer Trust Portal | Rubrik](#), and which Customer must comply with. Rubrik may suspend Customer's use of the AI Solutions upon Rubrik's reasonable determination that Customer is in breach of such different or additional Model terms.

THE AI SOLUTIONS ARE PROVIDED "AS IS" AND RUBRIK MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO (i) ANY OUTPUT OR ANY OTHER RESULTS THAT MAY BE OBTAINED FROM THE AI SOLUTION; (ii) ANY AI SOLUTION; (iii) ANY MODEL; OR (iv) THE ACCURACY OR LEGALITY OF ANY OTHER DATA OR INFORMATION OBTAINED THROUGH USE OF THE AI SOLUTIONS. THE AI SOLUTIONS ARE EXPRESSLY EXCLUDED FROM THE SERVICE LEVEL AGREEMENT AND RUBRIK'S INDEMNITY OBLIGATIONS IN THE AGREEMENT. NOTHING CONTAINED IN ANY OUTPUT WILL CREATE ANY WARRANTY NOT EXPRESSLY MADE HEREIN.

## RUBRIK SECURITY CLOUD – GOVERNMENT (“RSC-G”) PRODUCT SPECIFIC TERMS

The following product specific terms apply to Rubrik Security Cloud - Government (“**RSC-G**”).

### Definitions

- **“Classified Data”** means data that has been (a) categorized as ‘classified’ or ‘Classified National Security Information’ by the U.S. government, as defined in Executive Order 13526; or (b) is otherwise subject to U.S. government requirements including special clearance for use, access, or maintenance.
- **“Community”** means any individual or company that falls into one or more of the following: (a) a Government customer; (b) a non-Government customer or partner using RSC-G to provide solutions or outsource services to a Government customer; or (c) a non-Government customer or partner who uses RSC-G to manage data that is subject to Government regulations for which Customer determines, and Rubrik agrees, that the use of RSC-G is appropriate to meet regulatory requirements governing such data.
- **“Criminal Justice Information”** or **“CJI”** or **“CJIS”** has the meaning used in the Criminal Justice Information Services Security Policy.
- **“DFARS”** means Defense Federal Acquisition Regulation Supplement.
- **“DoD SRG”** means the Department of Defense Cloud Computing Security Requirements Guide.
- **“EAR”** means the Export Administration Regulations (15 CFR §§ 730-774).
- **“FedRAMP”** means the Federal Risk and Authorization Management Program (FISMA) (OMB Circular A-130) (FedRAMP Authorization Act of the National Defense Authorization Act)
- **“FedRAMP Authorized”** means a cloud service offering having achieved a marketplace decision as ‘FedRAMP authorized’ for a specific impact level as listed in the FedRAMP marketplace.
- **“Federal Tax Information”** or **“FTI”** has the meaning used in Internal Revenue Service Publication 1075.
- **“FERPA”** means the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g and 34 CFR Part 99)
- **“Government”** means a federal agency, state/local entity, or tribal entity acting in its governmental capacity.
- **“Heightened Standards”** means compliance requirements and frameworks imposed on Customer or Customer’s data by the Government such as HIPAA, PCI-DSS, HITECH, FedRAMP, State Authorizing Programs, ITAR, DFARS, CJI, FTI, StateRAMP, CMMC, or other similar heightened compliance standard.
- **“ITAR”** means the International Traffic in Arms Regulations (22 CFR §§ 120-130).
- **“U.S. Citizens”** has the meaning used in 42 USC § 9102(18).
- **“U.S. Persons”** has the meaning used in 22 CFR § 120.62.

### Product Overview

Rubrik’s RSC-G cloud service offering enables Customer to secure data in a Rubrik-hosted environment that has implemented, or attained certification for, certain information security and privacy standards such as FedRAMP, StateRAMP, DoD SRG, CJIS, and FERPA. RSC-G security or compliance certification posture may change over time with changes in Government regulations. Customer may elect to use RSC-G to secure data in a Customer-hosted or third-party licensed environment. In either case, such environment is Customer’s sole responsibility to manage, secure, and ensure compliance or certification with any Heightened Standards.

## User Access

Customer is responsible for verifying that its users accessing data managed by RSC-G are not prohibited by any applicable laws, regulations or restrictions from accessing such data.

## Export Control Regulations

Customer is responsible for complying with the EAR, ITAR, and any other export laws, regulations, or restrictions. Customer will ensure that any data managed by RSC-G is not exported or re-exported directly or indirectly in violation of, or used for any purposes prohibited by, such laws, regulations, or restrictions.

Customer is solely responsible for verifying that its users accessing data managed by RSC-G meet all applicable US Persons requirements prescribed by ITAR or any other export laws, restrictions, and regulations. Customer will restrict administrative access to the RSC-G environment to individuals that are U.S. Persons.

## Prohibited Workloads

Customer will not upload to, or manage any data with, RSC-G that (a) requires a higher certification level than attained by RSC-G; (b) is Classified Data; or (c) is subject to ITAR, EAR, DFARS 252.204-7010, DFARS 252.204-7012, or DoD SRG Impact Levels 4, 5 or 6 ((a) – (c) collectively are “Prohibited Workloads”) unless Customer has given Rubrik prior written notice, Rubrik has consented in writing, and the parties have agreed to any additional terms and conditions required by Rubrik.

Customer is solely responsible for all information spillage and sanitization costs incurred by Rubrik or its subcontractors, without application of any limitation of liability or damages caps in the Agreement, if Customer uses RSC-G for a Prohibited Workload or uses RSC-G in connection with data in violation of the Agreement, this Licensing Guide, or any applicable laws, regulations, or restrictions.

## Support Services

Rubrik’s Support Services provided by US Citizens on US soil are available to products within the regulated RSC-G boundary. RSC-G satisfies certain US regulatory requirements within the RSC-G boundary, but it also allows customers the flexibility to connect their existing non-regulated on-premise Rubrik Cloud Data Management (“**CDM**”) or RSC-Private (“**RSC-P**”) clusters to the regulated RSC-G boundary. If Customer elects to connect its regulated RSC-G environment to its on-premise CDM or RSC-P clusters that exist outside the regulated boundary, then Customer may receive follow-the-sun Support Services from non-US Citizens outside of the US for those Rubrik CDM or RSC-P clusters. It is within Customer’s sole discretion to connect its unregulated on-premise CDM or RSC-P clusters to its regulated RSC-G environment.

The Service Level Agreement in Exhibit A of the Agreement and the Response Time Targets in Section 7 of the Rubrik, Inc. Service and Software Support Policy do not apply to RSC-G due to its FedRAMP Authorized environment. Further, some Rubrik features, extensions and add-on offerings may not be compatible or certified for use with RSC-G (i.e. only specific Rubrik extensions are validated for the FedRAMP authorized environment). Customers can view Rubrik’s current uptime status for RSC-G at <https://status.rubrikgov.com>.

## FEDRAMP Secure Environment

The RSC-G service and the RSC-G support portal exists in a regulated environment that must only be accessible by permitted Customer individuals that are authorized members of the Community. Membership in the Community and access to the RSC-G service and the RSC-G support portal is at Rubrik’s discretion. Customer agrees to only use RSC-G and access the RSC-G support portal solely in Customer’s capacity as a member of the Community and for the benefit of Customer or another member of the Community. Use of RSC-G by an entity that is not a member of the Community, or to provide services to non-Community members, is strictly prohibited and could result in termination of Customer’s access to the RSC-G service and RSC-G support portal, penalties, or fines. If Customer uses RSC-G for data types requiring US citizenship or U.S. geographic location (i.e. continental United States), then Customer is responsible for ensuring that its RSC-G environment and the RSC-G support portal is only accessed by U.S. Persons within the United States. Customer may not share credentials with any non-Community individual or company. Customer is responsible for verifying its users are not prohibited by any applicable law or regulation and not subject to export control restrictions under U.S. export control laws and regulations. Customer may not use RSC-G for data located outside the continental United States regardless of whether such environment is Customer-hosted or Rubrik-hosted.

## Compliance

Customer’s use of RSC-G to comply with Customer’s Heightened Standards requirements may require additional controls to be implemented. Customer is solely responsible for implementing such additional controls and any applicable Customer-configurable security controls identified in the Customer Responsibility Matrix, including IP whitelisting and MFA for all user interactive logins (e.g.,



individuals authenticating to RSC-G) to protect Customer data subject to such Heightened Standards. Additionally, to the extent the Documentation or the Agreement sets forth specific requirements related to Heightened Standards, Customer must satisfy such requirements before providing Rubrik any Customer data subject to such Heightened Standards. If requested by Rubrik, Customer agrees to provide Rubrik with documentation sufficient to verify compliance with these RSC-G product specific terms.

Rubrik obtains information security and privacy compliance certifications, authorizations, and attestations that cover RSC-G and its associated Rubrik-hosted features and environment(s). Rubrik maintains an RSC-G CIS-CRM Workbook that provides a FedRAMP Controls Implementation Summary (CIS) and Customer Responsibility Matrix (CRM) that may be provided to Customer upon request. The RSC-G CIS-CRM Workbook is updated at least annually.

Due to the nature of backup services and encryption of Customer's data, the exact categories of data or Heightened Standards cannot be determined by Rubrik on Customer's behalf and may vary depending on Customer's use of RSC-G. Customer agrees that Rubrik has no obligation to assess the content, accuracy or legality of Customer's data, including to identify information subject to any specific Heightened Standard, legal, regulatory or other requirement. Customer is responsible for selecting and configuring the correct Rubrik product for its specific requirements and for making appropriate use of RSC-G to ensure a level of security appropriate to the particular content or classification of Customer data, including, where appropriate, implementation of encryption functionality, setting snapshot frequency, and data retention schedules.