

Barracuda Cloud-to-Cloud Backup SaaS Service Description

Barracuda sells products and services through channel partners to end users that use the products and services in their own business. For customers that purchase the Cloud-to-Cloud Backup SaaS Service offering (“**Service**”) from a Barracuda authorized channel partner, your use of the Service is subject to this Service Description and the [Barracuda Customer Terms and Conditions](#) (unless you have a negotiated agreement with Barracuda, in which case the negotiated agreement will apply).

Barracuda also sells the Service to managed service providers (“**MSP**”) for their use in connection with the managed services the MSP provides to its end customers. Such sale and use of the Service is subject to this Service Description and the MSP’s agreement with Barracuda under which the MSP purchases the Services. MSPs pass through to their end customers the Barracuda Customer Terms and Conditions (which incorporate this Service Description).

The applicable governing terms and conditions document and this Service Description together are referred to as the “**Agreement**.” This Service Description will govern if there is any conflict with other documents. Customers that purchase from an authorized channel partner and MSPs who purchase the Service are collectively referred to as the “**Customer**.” References to the “end customer” means the entity that benefits from use of the Service, regardless of purchasing methodology. Any capitalized terms used but not defined below have the meanings in the Agreement.

Overview

The Service provides easy, comprehensive backup and recovery for Microsoft 365 and Entra ID data, enabling customers to save a secure, encrypted backup of their Microsoft 365 and Entra ID data in a cloud environment. The Service provides the ability to back up and granularly recover data for the Exchange, OneDrive, SharePoint, Teams, OneNote applications, and Entra ID within Microsoft 365. The service also provides point-in-time recovery, and both scheduled and on-demand backup.

For more details about what data is backed up within the Service, see [Understanding What Data is Backed Up](#). For a list of features, improvements, and frequently asked questions (FAQs), see [Release Notes](#) and [Frequently Asked Questions \(FAQ\)](#).

Unit of Measure and Limitations

Unless stated otherwise, Barracuda sells subscriptions to the Service on a *per-user per month* basis. Customers must maintain a 1:1 ratio between users and licenses to the Service. Only one license is required per-user. Customers may transfer a user license from one user to another, but the prior user must completely stop using the Service. Customers may not allow multiple users to share a single license.

Microsoft 365

At the beginning of each backup, the Service will query which license each user has. Microsoft provides the Service with a list of user accounts in the customer's Microsoft tenant. If the user's Microsoft account is enabled and is provisioned with an active Microsoft 365 plan for one or more of Microsoft Exchange, OneDrive, SharePoint, or Teams, then the user requires a license for the Service. That user is then processed as a unique licensed user within the Service.

Entra ID

Barracuda sells subscriptions to Entra ID on a *per-member user per month* basis. A "member user" is a term used by Microsoft that includes employees of the customer but does not include a customer's guest users such as contractors, or non-human users, such as conference rooms. At the beginning of each backup, the Service will query which license each user has. Microsoft provides the Service with a list of user accounts in the customer's Microsoft tenant.

Reasonable Use

Your account is allocated a monthly data allowance of 300 GB ("**Data Allowance**") per license aggregated across a pool of storage for all licensed users. For example, if the customer has 3 licensed users, then the pool of storage for the entire customer account would be 900 GB. The customer will exceed its Data Allowance if all users, together, exceed the aggregate storage for its pool. This Data Allowance is provided to ensure that customers can effectively back up their essential data without encountering limitations. While the Service offers unlimited storage, customers must adhere to reasonable usage patterns. Barracuda reserves the right to charge for additional storage costs incurred. These charges will be applied to the customer's account based on the amount of excess data stored beyond the Data Allowance. Customers are expected to use the Service for legitimate backup purposes only. Any misuse, abuse, or illegal activities conducted through the Service are strictly prohibited and may result in immediate termination of the customer account.

Barracuda will notify the customer in advance if it is approaching or has exceeded the Data Allowance. This notification will serve as a warning to the customer to adjust its usage patterns accordingly to avoid additional charges.

For MSPs that would like to use the Service to manage their internal business data, the MSPs must acquire a separate subscription to the Service. MSPs must not co-mingle their internal business data with the data of any customer in the Service.

Data Privacy

Global Data Processing Addendum (DPA)

Barracuda's [DPA](#) provides both Barracuda's and its customers' rights and obligations regarding the processing of Customer Personal Data (as defined in the DPA) in connection with Barracuda's products and services. Barracuda's customers can electronically execute the DPA via our [Trust Center](#). For more information about how Barracuda processes personal data as a data controller, please review our [Privacy Notice](#).

Cross-Border Data Transfer

As a global company, Barracuda operates worldwide. When Barracuda receives or transfers personal data from the European Union, the UK, or Switzerland it does so in accordance with GDPR and local data protection laws. Where required, Barracuda leverages European Commission approved cross-border data transfer mechanisms including the EU's Standard Contractual Clauses incorporated into our DPA. For data transfers to the United States, Barracuda is self-certified under the US Department of Commerce Data Privacy Framework, and its certification can be found [here](#).

Data Retention

At the expiration or termination of the Service, Barracuda generally stores customer data for 30 days post termination to allow additional time for customers to manually export their data or renew the subscription. After this 30-day retention period, Barracuda will fully disable the account and commence deletion of all customer data, including any cached or backup copies.

Barracuda does not offer a data export service for the Service. If a customer does not plan to renew its subscription and needs to access its backup data, Barracuda recommends that the customer plan accordingly and begin the process of exporting its data as needed prior to the end of the retention period.

Location of Customer Data

The Service is offered on the Microsoft Azure cloud infrastructure. See the *Security – Data Center Locations* section below for more information.

Three types of data are collected by the Service: the customer's files, metadata about the customer's files, and operational logs about the Service. Customer files and associated metadata live and remain in the region the customer selects. Log data resides in the US. All 3 data types are encrypted at rest and in transit—see *Data Transmission and Storage* below for more information.

Barracuda does not have access to customer files or associated metadata. If a customer opens a support ticket and turns on the support tunnel, then Barracuda could potentially see the customer files and associated metadata. Barracuda provides support using its follow-the-sun support process.

Data Transmission and Storage

The Service maintains immutable backup copies by preventing direct access to the data as well as protecting against data modification or removal via API. For more information about how the Service protects the data, please see

<https://campus.barracuda.com/product/cloudtocloudbackup/doc/96020206/how-barracuda-cloud-to-cloud-backup-can-protect-you-from-ransomware/>.

The Service encrypts all data in transit and at rest. Customer data remains encrypted until it is requested for a restore. Customer data stored in the Service is written once and never updated.

Security

Access Control

To provide the flexibility to limit access to their account, customers can use the Barracuda Cloud Control interface to access and manage their Service accounts. You can read more about how to set roll-based access at:

<https://campus.barracuda.com/product/cloudtocloudbackup/doc/167578170/settings-page>.

The Service supports multifactor authentication. Additional information about this feature is available at:

<https://campus.barracuda.com/product/cloudcontrol/doc/69960137/multi-factor-authentication-in-barracuda-cloud-control>.

Barracuda personnel may only access customer data at rest in certain circumstances including, for example, to provide support where access is necessary to address the customer's concerns and request.

Data Transmission and Storage

The Service secures data transfers using HTTPS. Those parts are AES 256-bit symmetrically encrypted, are written into storage in an encrypted state and remain encrypted until requested for restore.

If customer data needs to be restored for any reason, the Service will scan for malicious content before conducting the restoration to help prevent the customer data from becoming infected again. Customers can read more about this feature at: <https://campus.barracuda.com/product/cloudtocloudbackup/doc/358941563/malware-scanning-during-restore>

Data Center Location

Barracuda maintains a network of datacenters by geographic location around the globe and requires that each meet defined security requirements. The cloud infrastructure for the Service is deployed in various geographical regions. Barracuda stores customer data at rest in the region customer selects at the time of initial product configuration.

Americas:

- Microsoft Azure Region - East US 2 (Virginia)
- Microsoft Azure Region - Canada Central (Toronto)

EMEA:

- Microsoft Azure Region - UK South (London)
- Microsoft Azure Region - Germany West Central (Frankfurt)
- Microsoft Azure Region - West Europe
- Microsoft Azure Region - France Central (Paris)
- Microsoft Azure Region - Switzerland North (Zürich)
- Microsoft Azure Region - Sweden Central (Gavle)
- Microsoft Azure Region - UAE North (Dubai)
- Microsoft Azure Region - South Africa North (Johannesburg)

APAC:

- Microsoft Azure Region - Australia East (New South Wales)
- Microsoft Azure Region - Japan West (Osaka)
- Microsoft Azure Region - Central India (Pune)

Operations and Organizational Controls

Barracuda employees are expected to be competent, thorough, helpful, and courteous stewards of customer data that is stored on the Service. Barracuda has established a number of measures to ensure that customers and their data are treated properly.

New Hires and Orientation

All new employees are required to accept and acknowledge in writing Barracuda's policies for non-disclosure and protection of Barracuda and third-party confidential information, including acceptable use of confidential information. When assisting customers with their technology solutions, Barracuda support technicians understand that they may come into contact with customer communications and/or customer data, and they are not to view the contents of that email without explicit permission from the customer. Barracuda employees are not to disclose the contents of that customer email to a third party under any circumstances.

New technical support employees are provided a job description and expectations when hired regarding maintaining the confidentiality and security of customer email.

Training

Technicians who support the Service are prepared in a variety of ways. New tier 1 technicians receive class time training with tier 2 technicians and the support management team. New support technicians also spend time as understudies to an established technician for each product in which they intend to become certified. All Barracuda support technicians receive ongoing training in product-specific training sessions.

Oversight

Access to the Service is limited to approved Barracuda personnel on an ‘as needed’ basis. Each tier 1 technician is attended by and reports to or is mentored by a tier 2 or tier 3 technician. Each tier 2 or, when applicable, tier 3, is responsible for no more than four tier 1 technicians. Support for the Service is provided from all our support regions. Support calls from customers in the United States are generally handled by technicians in the United States. Support calls from customers outside the United States could be routed to any of these facilities. When an employee or contractor leaves Barracuda, a formal process is in place to immediately revoke physical and network access to Barracuda facilities and resources.

Use of Artificial Intelligence

The Service does not use Artificial Intelligence. (AI)

The Service is not intended for use in situations that would cause the Service to be considered “High-risk AI” under the EU AI Act. Customers must not use the Service in a manner that would subject Barracuda to obligations applicable to High-risk AI. Barracuda may terminate the customer’s applicable subscriptions to the Service if it violates this obligation. Barracuda has no responsibility for customers’ use of the Service in situations considered “High-risk AI.”

Termination of the Service and Data Export

Barracuda will retain customer data for 30 days after the date of expiration of the customer’s subscription. This is a grace period during which a customer can renew their subscription and is intended to provide for inadvertent failures to renew. From days 31-45, the customer data within the Service becomes read-only and will not accept any further data for backup. At this time the customer data remains available for export or to restore a customer’s production environment. From days 46-60, the Service features are no longer available. At day 60, Barracuda will begin automatically deleting the customer data. After the 60-day

period, Barracuda will have no obligation to maintain or provide any customer data and will have no liability resulting from destruction of the customer data.

Service Redundancy, Back Ups, and Disaster Recovery

The Service stores customer data on the Microsoft Azure cloud infrastructure. Azure Storage stores multiple copies of customer data to protect it from planned and unplanned events. Examples of these events include transient hardware failures, network or power outages, and natural disasters. Redundancy ensures that the customer storage account meets its availability and durability targets even in the face of failures.

Customer data in an Azure Storage account is replicated 3 times in the primary region. Azure Storage offers 2 options for how customer data is replicated in the primary region:

- **Zone-redundant storage (ZRS)** copies customer data synchronously across 3 Azure availability zones in the primary region.
- **Locally redundant storage (LRS)** copies customer data synchronously 3 times within a single physical location in the primary region.

The Service uses ZRS in all regions where ZRS is supported by Microsoft Azure. In regions where ZRS is not supported by Microsoft Azure, locally the Service uses LRS.

Service Level Agreement (“SLA”)

Barracuda makes the following 2 commitments to customers in connection with use of a paid subscription to the Service that has not been suspended for any reason.

1. **Data Backup:** Subject to the Exceptions stated below, Barracuda agrees that you will be able to replicate data to the Service 99.9% of the time each calendar month, provided that you have purchased the relevant subscription from Microsoft - 365 Exchange Online, OneDrive for Business, SharePoint, Teams, or Entra ID (**“Data Backup Commitment”**).
2. **Web Access:** Subject to the Exceptions stated below, Barracuda agrees that you will be able to access the management console for the Service at least 99.9% of the time each calendar month (**“Web Access Commitment”**).

Exceptions. The above commitments are subject to the following exceptions: (a) planned downtime or emergency maintenance for the Service; and (b) any unavailability caused by: force majeure event; actions/inactions by persons other than Barracuda and its contractors; third-party products or services used with the Service; outages that are less than 5 continuous minutes in duration (e.g., monitor connectivity glitches); Internet, hosting or

platform service provider failure or delay; denial of service attack; use of the Service in violation of the Barracuda Customer Terms and Conditions; or use of Service that is not in accordance with Documentation (as defined in the Customer Terms and Conditions) (collectively “**Exceptions**”).

Reporting and Calculating Excess Downtime. Certain Barracuda products display uptime information at <https://status.barracuda.com/>. Any Service-impacting condition that you experience must be reported within 24 hours to [Barracuda Networks Support](#), and, if required by Barracuda, you must provide Barracuda Networks Support with access to your Service account and any applicable on-premises Barracuda Networks equipment. For calculating the amount of excess downtime, over the relevant Barracuda commitment, the downtime does not begin until you report the Service-impacting condition to Barracuda Networks Support.

Barracuda Trust Center

The Barracuda Trust Center is located at <https://trust.barracuda.com/>. Barracuda periodically updates the Trust Center. The then-current version of the Trust Center governs.

At the Trust Center customers can find the following, among other information:

- Product Certifications : <https://trust.barracuda.com/security/certifications>
- Security advisories: <https://trust.barracuda.com/security/information#security-advisories>
- Trade Compliance information and certain applicable forms: <https://trust.barracuda.com/legal/trade-compliance>
- Frequently requested documents, such as Certificate of Insurance, Business Associate Agreement, Non-disclosure Agreement, copy of the current SOC2 report, privacy documents, and more.

Discontinuation of Services

Barracuda will provide distributors, resellers, and other customers reasonable notice before discontinuing sale of the Service (or associated material functionality) unless Barracuda replaces such discontinued Service or functionality with a materially similar Service or functionality. Nothing in this section limits Barracuda’s ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This section does not apply to pre-general availability Services, offerings, or functionality.