

Barracuda Email Gateway Defense 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 Barracuda Email Gateway Defense service offering (“**Service**”) from a Barracuda authorized channel partner, your use of the Service is subject to this Service Description and the Barracuda Legal 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. When an MSP provides its end customer with direct access to the Service, the 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.

Contents

Contents 1

OVERVIEW..... 1

UNIT OF MEASURE AND LIMITATIONS..... 1

SERVICE LEVEL AGREEMENT (“SLA”)..... 2

DATA PROTECTION AND SECURITY 3

BARRACUDA IQ™ – ARTIFICIAL INTELLIGENCE (“AI”)..... 5

CUSTOMER PROVIDED THIRD PARTY SOFTWARE..... 5

END OF SALE AND END OF SUPPORT 6

OVERVIEW

Barracuda's cloud-hosted Email Gateway Defense leverages advanced threat detection and prevention technologies to protect customers from spear phishing, ransomware, and other email-borne threats. As a SaaS solution, the Service lets customers focus on what matters while Barracuda manages and updates their email security.

UNIT OF MEASURE AND LIMITATIONS

Please see the licensing measurements and restrictions published on Barracuda Campus at <https://campus.barracuda.com/product/campus/doc/172891718/license-definitions-email-protection-products/>.

The Service is sold on a per seat basis. Customer must maintain a 1:1 ratio between users and licenses to the Service. Per-seat licenses may be transferred from one user to another only when the original user no longer requires the license (for example, due to role change or departure).

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.

A customer's use of the Service may be subject to additional or different restrictions as specified in the applicable Barracuda quote (for example, without limitation, the quote may limit users to a particular geography or to a particular legal entity, or to a defined number of administrative users).

SERVICE LEVEL AGREEMENT ("SLA")

Barracuda publishes Service status updates at <https://status.barracuda.com>. Barracuda makes the following commitments to customers in connection with use of a paid subscription (and not merely a free trial) to the Service that has not been suspended for any reason.

Email Delivery Commitment. Barracuda agrees that customers will be able to deliver email messages to and from the Service email servers at least 99.9% of the time each calendar month ("**Email Delivery Commitment**"). The Email Delivery Commitment will not apply to the following circumstances:

- Emails containing attachments that cannot be scanned (i.e., encrypted or password-protected attachments).

- Implementation by customer of excessively complex full-text content policies.
- Emails sent by customer to large external distribution lists, which may be subject to serialized delivery.
- Customer or third-party inability to access the primary or backup MX host servers due to a failing in the Internet.
- Viruses introduced to customer's systems by customer.
- Problems caused by mail servers that are not RFC-822 compliant.
- Where customer's email system appears to be operating as an "open relay." "Open relay" means an email server configured to receive mail from an unknown or unauthorized third party and forward mail to recipients who are not users of that system.

Web Uptime Commitment. Barracuda agrees that customers will be able to access the management console for the Service at least 99.9% of the time each calendar month ("**Web Uptime Commitment**"), provided that downtime or outages related to any server on the Internet, customer premise equipment, transportation of data across the Internet, or any periods during scheduled or emergency maintenance windows or customer-requested service interruptions are not included within the scope of, and are excluded from, this availability 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 events, 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, 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 the Service that is not in accordance with Documentation (collectively "**Exceptions**").

Service-impacting conditions must be reported to Barracuda Support within twenty-four (24) hours of the event. If required, customers must also grant access to their Service account and any related on-premises Barracuda equipment. Downtime calculations begin once the issue is reported.

DATA PROTECTION AND SECURITY

Data Privacy Terms. Barracuda's Global 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. Barracuda operates worldwide. When Barracuda receives or transfers personal data it does so in accordance with local data protection laws, like the GDPR, for example. Where required, Barracuda leverages European Commission approved cross-border data transfer mechanisms including the EU's Standard Contractual Clauses incorporated into our DPA. For personal data transfers to the United States, Barracuda is self-certified under the US Department of Commerce Data Privacy Framework.

Access Control. Customers can configure user roles to manage access privileges manually or by integrating user authentication via LDAP or Microsoft Entra ID (formerly Azure AD). Barracuda support access to the Service is limited to approved Barracuda personnel on an as-needed basis.

For customers whose data is stored at rest in any non-US data center location, please see Barracuda's discussion regarding the 2018 US CLOUD Act.

Data Retention During Subscription Period. The Service captures incoming and outgoing messages as the comprehensive record of activity and provides information about each customer's current configuration and policy settings within the Service. The Service maintains up to thirty-two (32) days of log files and associated messages at any time. These log files and any associated messages are purged from the Service on a rolling basis.

Data Center Security and Data Residency. The Service is offered on the Amazon Web Services (AWS) cloud infrastructure. The data center provider's compliance documentation is at [AWS Trust Center](#).

Barracuda stores customer data at rest in the region the customer or its representative selects from the available regions below.

Americas

- AWS Region – US East-2 (Ohio)
- AWS Region – ca-central-1 (Canada)

EMEA

- AWS Region – EU West-2 (London)
- AWS Region – EU Central-1 (Frankfurt)

APAC

- AWS Region – AP Southeast-2 (Sydney)
- AWS Region – AP South-1 (Mumbai)

Back Ups and Disaster Recovery. For Barracuda’s AWS environment, Barracuda maintains a comprehensive data backup policy to support business continuity and disaster recovery best practices. Data backups are taken daily.

Data Transmission. The Service secures data transfers using HTTPS. Emails from the customer or sender’s mail server are transmitted to one data center and then replicated to another. Customer data transmitted through the Service is encrypted in transit and at rest using industry-standard encryption. To ensure high availability and data durability, the Service stores and replicates data across multiple secure Barracuda-operated or -managed data center locations. With this architecture, the Service may maintain up to three distinct copies of customer data, each stored in the cloud.

Subscription Termination and Data Export. Barracuda generally stores customer data for thirty (30) days post termination or expiration of a subscription to allow additional time for the customer to export its data. After the thirty-day period, Barracuda will have no obligation to maintain or provide any customer data and will have no liability resulting from the destruction of the customer data. The Service allows customers to export their data at any time during the subscription term.

BARRACUDA IQ™ – ARTIFICIAL INTELLIGENCE (“AI”)

Use of AI. This Service uses AI services from Barracuda IQ to enhance the effectiveness and efficiency of the Service. Please see the [Barracuda IQ Service Description.pdf](#) to read more about how Barracuda uses AI in the Service.

No High-Risk AI Systems. 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.”

CUSTOMER PROVIDED THIRD PARTY SOFTWARE

In situations where Customer wishes to use third party software to interoperate with the Service, Customer grants Barracuda permission to allow the third party and its provider to access customer data through the Service in accordance with their terms of use and any specific permissions Customer establishes. Customer is responsible for the acts and omissions of any such third party with respect to customer data accessed through the Service.

END OF SALE AND END OF SUPPORT

See the Barracuda [End of Sale and End of Support Policy](#) on the Trust Center. Nothing in this section limits Barracuda's ability to make changes required to comply with applicable law, address a material security risk, or avoid substantial economic or material technical burdens. This section does not apply to pre-general availability Services.