# Barracuda Essentials for Email Security

Data Protection and Security

# TABLE OF CONTENTS

# Overview

This document walks through security measures in place to protect customer email stored by Barracuda Email Security Service. The process begins at the cloud service and ends at the datacenter. This document includes a description of the facilities that host email protected by Barracuda Email Security Service and descriptions of operational and organizational controls enforced by Barracuda Networks.

# 1. Product Security

## 1.1 Barracuda Email Security Service

Barracuda Email Security Service supports 256-bit TLS connection for email transmission.

The Barracuda Email Security Service is deployed in the cloud and uses https over port 443 with a 256-bit encryption for administration.

The Barracuda Email Security service runs on a Linux kernel. In the event that a security flaw is discovered, updates are pushed out to Barracuda Email Security Service cloud.

# 2. Data Transmission and Storage

## 2.1 Storage Facility Standards

Barracuda Networks leases space in a number of Tier 3 & 4 datacenters worldwide. Each Barracuda Networks datacenter is equipped with:

- Controlled access systems requiring key-card authentication.
- Video-monitored access points
- Intrusion alarms.
- Locking cabinets.
- Climate Control systems.
- Waterless fire suppressant systems
- Redundant power (generator backup, UPS, no single point of failure)
- Redundant Internet connectivity

## 2.2 Data Storage

Email is transmitted from the customer or senders mail server to one datacenter and then replicated to another. Email in the cloud is stored on different servers, and each of these servers retains email files. This diverse storage system serves to further strengthen the physical security of customer email.

With this architecture, Barracuda Email Security Service can maintain up to three distinct copies of customer data. Each of these copies is stored in the cloud.

## 2.3 Data Locations

Barracuda maintains a network of datacenters by geographic location around the globe and requires that each meet defined security requirements. The cloud infrastructure for Barracuda Email Security Service is deployed in the following geographical regions. Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the European Union will be done in compliance with the GDPR and applicable local privacy laws. Barracuda's Standard Contractual Clauses are located within our DPA at the following address: https://www.barracuda.com/company/legal/trust-center

**US**

- AWS Region - US East – 2

**CA**

- AWS Region - Ca-Central-1

**UK**

- AWS Region – EU West - 2

**DE**

- AWS Region – EU Central – 1

**AU**

- AWS Region – AP Southwest -2

# 3. Operations and Organizational Controls

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

## 3.1 New Hires and Orientation

All new employees are required to accept and acknowledge in writing Barracuda Networks' policies for non- disclosure and protection of Barracuda and third-party confidential information, including acceptable use of confidential information. In the course of 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 Networks 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.

## 3.2 Training

Technicians who support Barracuda Email Security 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 a period of time as understudies to an established technician for each product in which they intend to become certified. All Barracuda Networks support technicians receive ongoing training in product-specific training sessions.

## 3.3 Oversight

Access to Barracuda Email Security Service servers is limited to approved Barracuda Networks personnel on an ‘as needed’ basis. Each tier 1 technician is attended by and reports to a tier 2 technician. Each tier 2 is responsible for no more than four tier 1 technicians. Support for Barracuda Email Security 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 Networks facilities and resources.