# Barracuda PhishLine

Email Protection and Security

# TABLE OF CONTENTS

# Overview

This document describes product security measures and data storage policies that are specific to the Barracuda PhishLine. PhishLine helps you guard against a range of threats with patented, highly-variable attack simulations for multiple vectors, including phishing, smishing, vishing, and found physical media.

# 1. Product Security

## 1.1 Barracuda PhishLine Service

PhishLine and its customers utilize the PhishLine Administrative Web Site. The website only supports a secure HTTPS connection, requiring TLS 1.2 and supporting TLS 1.3. Due to the customizability of the solution, other external connections may take advantage of other types of encryption (e.g. SFTP) to transmit data.

# 2. Data Transmission and Storage

## 2.1 Storage Facility Standards

Barracuda Networks leases space in a number of Tier 3 & 4 datacenters in the US. 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 Access, Transmission and Storage

Barracuda PhishLine maintains campaign data after the customer has completed the training. The campaign data is transited over a TLS encrypted connection. The data is stored and kept encrypted in secure locations accessible only by select individuals from PhishLine team. Additional technical and security controls are in place to protect the customer data derived from the campaigns results. In every case, rigorous technical and security controls are in place to protect these files and systems. All computer systems exist in protected data centers that utilize both physical and electronic access controls, all access is monitored and audited.

## 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 PhishLine 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

- Colocation: US East (Illinois and Wisconsin)

# 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 services 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 data without explicit permission from the customer. Barracuda Networks employees are not to disclose the contents of that customer data 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 data.

## 3.2 Training

Technicians who support the Barracuda PhishLine are prepared in a variety of ways. New technicians receive class time training with senior technicians and the support management team. New support technicians also spend a period of time as an understudy 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

Support for Barracuda PhishLine is provided out of United States.

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