Barracuda Managed Workplace

Data Privacy Overview

Last Updated May-2020 • US 1.0 • Copyright 2020 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com

Overview

This document describes data privacy measures and data storage policies that are specific to Barracuda Managed Workplace.

Barracuda is dedicated to protecting our customers' privacy and helping them protect the privacy of their users and customers. Our products help customers comply with global, regional, and national privacy regulations, including technical requirements of the General Data Protection Regulation (GDPR).

Barracuda Managed Workplace is a complete remote monitoring and management (RMM) platform with robust, integrated security tools and services. With Managed Workplace RMM, IT service providers can quickly assess vulnerabilities, secure weak points, monitor anomalies, and seamlessly recover data in the event of an attack - all from a single dashboard.

Data Inventory, Data Protection Impact Assessment (DPIA), and Data Mapping

Barracuda has conducted and maintains a data inventory and data mapping of the collection, transfer, and storage of Personal Information for Barracuda Managed Workplace. Further, the required Data Protection Impact Assessment (DPIA) for applicable controls has been completed and safeguards are in place to mitigate potential risks.

Customer Consent

Barracuda's Data Processing Addendum sets forth each party's rights and obligations with regard to the processing of personal data. Barracuda's Data Processing Addendum for data controllers can be executed on our Trust Center within the Self Service Center at the following address:
https://www.barracuda.com/company/legal/trust-center

Cross-Border Data Transfer

Barracuda complies with the EU – US cross-border data transfer mechanisms approved by the European Commission regarding the collection, use, and retention of Personal Information transferred from the European Union to the United States. 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

Employee Training

Upon hire and annually thereafter, Barracuda employees who have access to customer data undergo security and data privacy awareness training to ensure their continued knowledge of obligations and responsibilities to comply with data protection requirements.

Retention and Right to Be Forgotten (RTBF)

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

If you wish to send a Right to Be Forgotten (RTBF) request, please send an email to legal@barracuda.com and Barracuda will provide timely updates through the process of data deletion.

Data Transmission and Storage

Onsite Managers and Device Managers communicate to the Service Center via TLS encryption. The Onsite Manager or Device manager will initiate an outbound connection over the standard TLS port (443). Similarly, only port 443 is allowed inbound to the Service Center servers. This is locked down by traditional firewalls and AWS security groups.

Sensitive data including Service Center login passwords and credentials used to monitor and manage devices are secured using AES 256-bit encryption.

Access Control

Partners can configure user roles and permissions to define the level of access users have to the Service Center. In addition to using standard usernames and passwords to login to the Service Center, partners can enable Multi-Factor Authentication and/or Single Sign-On for added protection. Each login access to Service Center is recorded in an audit log that the partner can access. More information about these features is available at the following address:
https://campus.barracuda.com/product/managedworkplace/doc/91129500/setting-up-user-accounts

Data Location

Barracuda maintains a global network of data centers and annually verifies that each one meets defined security and privacy requirements. The cloud infrastructure for Barracuda Managed Workplace is deployed in the Americas, EMEA, and APAC regions via AWS. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws.