Barracuda MSP (Intronis Backup)

Protection and Security

TABLE OF CONTENTS

Overview **3**

Audience **3**

Storage Facility Standards **3**

Data Locations 4

Data Access **4**

Access by Barracuda MSP Personnel 4

Limits to Access 4

Data Transmission and Data Storage **4**

Data Portability 4

Data Retention 5

Operations and Organizational Controls **5**

New Hire Orientation 5

Training 5

Oversight 5

Overview

This document provides a description of the product security measures and data storage policies specific to the Barracuda MSP Intronis Backup (IBU).

The following information is included:

- Audience
- Barracuda MSP Intronis Backup
- Storage Facility Standards
- Data Location
- Data Access
- Data Transmission and Data Storage
- Operations and Organizational Controls

Audience

This document is intended for IT professionals and partners providing their clients with Barracuda MSP data backup and security services.

Barracuda MSP Intronis Backup

Barracuda MSP Intronis Backup is a software-only backup and disaster recovery (BDR) solution designed to protect critical data. Built specifically for MSPs around a centralized management portal, IBU enables you to protect, recover, and restore SMB files, folders, emails, applications, and servers — physical or virtual — both locally and in the cloud.

Storage Facility Standards

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

- Controlled access systems requiring keycard authentication (Somerville requires keycard and fingerprint 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

Data Locations

Barracuda MSP Intronis Backup data is stored in the following regions.

Americas

- US-East: Somerville, MA
- US-West: Los Angeles, CA
- Canada: Toronto, ON

EU

- UK: Reading

Note: Data is stored or failed-over in the region where the customer has set up the corresponding Barracuda MSP solution.

Data Access

The Barracuda MSP Intronis Backup (IBU) can be managed in the following ways:

- Customers can use the Barracuda MSP web interface to securely manage the Barracuda MSP Intronis Backup Service features.
- Customers can configure user roles to determine the level of access to the Barracuda MSP Intronis Backup service.
- Barracuda MSP employees can log-in and manage the Barracuda MSP Intronis Backup Service using strong authentication and VPN tunnels.

Access by Barracuda MSP Personnel

Barracuda MSP personnel are granted access only when necessary under management oversight. Barracuda MSP personnel use customer data only for purposes compatible with providing you the services, which can include customer support and troubleshooting.

Limits to Access

The operational processes and controls that govern access to and use of customer data in the Barracuda MSP Cloud are regularly verified. Barracuda MSP regularly performs sample audits to attest that access is for legitimate business purposes only. Strong controls and authentication limit access to customer data to authorized personnel only. When access is granted, whether to Barracuda MSP personnel or to our subcontractors, it is carefully controlled and logged, and revoked when longer needed.

Data Transmission and Data Storage

The Barracuda MSP Intronis Backup service encrypts protected files with AES 256-bit symmetrical encryption and securely transmits the data to the Barracuda MSP Cloud. The protected data remains encrypted until restored.

Data Portability

You can retrieve a copy of your customer data at any time and for any reason without any assistance or notification required from Barracuda MSP.

Data Retention

If you, the customer, terminate your subscription or it expires (except for free trials), Barracuda MSP stores your customer data in a limited-functional account for 30 days (the retention period) to give you time to export the data or renew your subscription.

Operations and Organizational Controls

Barracuda MSP employees are expected to be competent, thorough, helpful, and courteous stewards of customer data stored in the Barracuda MSP data centers. Barracuda MSP has established the following measures to ensure that customers and their data are treated properly:

- New Hire Orientation
- Training
- Oversight

New Hire Orientation

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

In the course of assisting customers with their technology solutions, Barracuda MSP support technicians understand that they may be exposed to customer communications and/or customer data and they are not to view the contents of that data without explicit permission from the customer. Barracuda MSP 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.

Training

Technicians who support Barracuda MSP Intronis Backup are trained 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 MSP support technicians receive ongoing training in product-specific training sessions.

Oversight

Support for Barracuda MSP Intronis Backup is provided from the United States and the United Kingdom.

Technicians in the United States generally handle support calls from customers in the United States. Support calls from customers outside the United States may be routed to any of these facilities.

When an employee or contractor leaves Barracuda MSP, a formal process is in place to immediately revoke physical and network access to Barracuda MSP facilities and resources.